Deep-Learning-Based Blockchain for Secure Zero Touch Networks

Randhir Kumar, Prabhat Kumar, Moayad Aloqaily, and Ahamed Aljuhani

The authors analyze the attack surface on IoT-enabled ZTNs and the inherent architectural flaws for such threats. After an overview of attack surface, the article presents a new deep-learning- and blockchain-assisted case study for secure data sharing in ZTNs.

Abstract

The recent technological advancements in wireless communication systems and the Internet of Things (IoT) have accelerated the development of zero touch networks (ZTNs). ZTNs provide self-monitoring, self-configuring, and automated service-level policies that cannot be fulfilled by the traditional network management and orchestration approaches. Despite the hype, the majority of data exchange between participating entities occurs over insecure public channels, which present a number of possible security risks and attacks. Toward this end, we first analyze the attack surface on IoT-enabled ZTNs and the inherent architectural flaws for such threats. After an overview of attack surface, this article presents a new deep-learning- and blockchain-assisted case study for secure data sharing in ZTNs. Specifically, first, we design a novel variational autoencoder (VAE) and attention-based gated recurrent units (AGRU)-based intrusion detection system (IDS) for ZTNs. Second, a novel authentication protocol that combines blockchain, smart contracts (SCs), elliptic curve cryptography (ECC), and a proof of authority (PoA) consensus mechanism is developed to improve secure data sharing in ZTNs. The extensive experimental results show the effectiveness of the proposed approach. Lastly, this work discusses critical issues, opportunities, and open research directions to solve these challenges.

Introduction

Next-generation networks and futuristic technologies have the potential to revolutionize the present wireless ecosystem using advanced supporting technologies such as software-defined networking (SDN), intelligent blockchain, and edge intelligence [1]. The network infrastructure and supporting technologies are developed to meet the ever increasing demands of three new service categories, each with its own set of requirements of efficiency, reliability, and low-latency communications [2]. Despite significant enhancements, the current conventional wireless ecosystem does not fulfill the next-generation network capabilities including ultra-low latency, mobility support, and seamless connection with high reliability [3]. This restriction is primarily caused by the fact that a typical network infrastructure is made up of different terrestrial and non-terrestrial components, including the Internet of Things (IoT), mobile devices, small cells and macrocells, satellites, and unmanned aerial vehicles (UAVs) [4]. As a result, offering fully automated network operations and monitoring the network using current network management and orchestration (MANO) technologies is challenging and unreliable [5]. In order to overcome these limitations, the network infrastructure probably requires novel solutions, and capabilities to ensure autonomous and efficient resource management, and appropriate end-to-end quality of experience (QoE) for end users. The use of the European Telecommunications Standards Institute (ETSI)'s zero touch networks (ZTNs) and associated service management present a significant solution to make the vision of fully automation of the network a reality [6]. Figure 1 shows the various benefits of ZTNs that are achieved by automating and distributing the core network functions.

The ZTN framework is envisioned as a next-generation system that intends to perform all operational procedures and activities (e.g., planning and design, delivery, deployment, provisioning, monitoring, and optimization) automatically, preferably without human interaction [7]. The usage of ZTNs offers network management solutions with implicit security. However, the majority of contemporary security threats are linked to the growing number of IoT devices and the usage of cloud-based and edge-based services in ZTNs. For example, IoT devices can easily be compromised by an attacker as they are physically deployed in ZTNs without any security measures [8]. Moreover, several security and privacy breaches are possible in the network as the communication takes place through an insecure channel [9]. Thus, the entire system can be compromised, and an adversary can perform several attacks including modification of data, exploitation of exchanged and stored information in ZTNs, man-in-the-middle, replay, impersonation, and session key (SK) disclosure attacks [10]. This necessitates exploring optimized solutions to combat the aformentioned threats and attacks on ZTNs.

Motivation of Blockchain and Deep Learning

Blockchain and deep learning (DL) have the potential to solve many challenges of ZTNs in an efficient manner. For instance, blockchain provides a decentralized mechanism that ensures reliability, trust, and transparency with confidentiality, integrity, and availability (CIA) compatibility for serving future ZTN application. This is done particularly by performing the standard procedures: ini-

Digital Object Identifier: 10.1109/MCOM.001.2200294

Randhir Kumar is with SRM University AP, India; Prabhat Kumar is with LUT University, Finland; Moayad Aloqaily is with Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE; Ahamed Aljuhani is with the University of Tabuk, Saudi Arabia.

tiating the transaction, broadcasting and verifying it, creating and validating the new blocks using a consensus method, and last, updating the blockchain ledger. These functions are implemented on top of several other security techniques such as cryptography, hashing, and peer-to-peer (P2P) networking [13]. Moreover, when compared to centralized servers, blockchain-enabled networks provide a trusted and authentic execution setup to ensure permissible access to the system and data. The functionality of blockchain can also be maximized by introducing smart contracts, which are algorithms of actions taken on particular agreed-upon events [10].

On the other hand, DL has the capability to learn heterogeneous, unstructured, and large volumes of ZTN data. Additionally, this is advantageous since learning is accomplished automatically (i.e., without human interaction) to extract hidden patterns from large-scale data. In the context of ensuring network security, intrusion detection systems (IDSs) can be developed or deployed at a strategic point within the network to tackle unseen malicious transactions. An IDS is typically used to recognize network traffic, particularly to differentiate between legitimate and malicious traffic, and is therefore helpful in getting rid of unwanted traffic. DL-based IDSs can improve overall accuracy and can be easily generalized when compared to machine learning (ML)-based IDSs. In this direction, there are very few research articles that have examined the vulnerabilities of upgrading ZTNs from traditional networks, and research work on developing solutions for secure data sharing based on blockchain and DL, particularly for ZTNs, is still in its infancy. For instance, articles presented in [2, 3, 5, 9, 11] provided scattered ideas or frameworks of using ML or DL-based IDSs in ZTNs. However, detecting intrusion with standalone ML- or DL-based IDSs is challenging as most ZTN applications have longer sequences of time-series data, and also have a large number of features (due to their nonlinear and non-stationary characteristics) with multiple layers. A few works presented, such as [8], either used blockchain for storing entire transactions or just surveyed generic ways to include blockchain in ZTNs. Furthermore, storing entire transactions on blockchain has proved to be quite inefficient and costly. Table 1 shows the comparison of existing solutions for ZTNs.

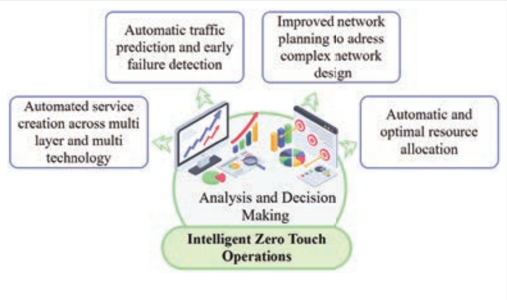
Automatic traffic prediction and early failure detection
Improved network planning to adress complex network design
Automated service creation across multi layer and multi technology
Automatic and optimal resource allocation
Analysis and Decision Making
Intelligent Zero Touch Operations

FIGURE 1. Advantages of ZTNs by automating the core network functions.

Contributions and Organization

Motivated by the aforementioned challenges, this article discusses potential attack surfaces on IoT-enabled ZTN systems, as well as recommended practices for dealing with those challenges using blockchain and DL:

- Specifically, we have designed a DL-based IDS that combines a variational autoEncoder (VAE) with attention-based gated recurrent units (AGRUs). The VAE is used to extract the features automatically, thus eliminating the requirement for domain-specific knowledge. Moreover, it is trained in an unsupervised manner to automatically extract features. The extracted features are used by the AGRU model to detect intrusion. We made use of the attention mechanism to assign different weights to spatial and temporal features, since assigning equal weights can hamper the entire intrusion detection process. Moreover, the GRU eliminates the vanishing gradient problem and runs faster computation than standard recurrent neural network (RNN) layers to its two gate structure.
- The blockchain scheme first adopts an authentication and access control mechanism based on elliptic curve cryptography (ECC) to establish a session key between the participating entities of ZTNs. The block verification process is performed using a smart contract-based proof of authority (PoA) consensus mechanism. The proposed approach reduces the storage cost and throughput to access ZTN data by storing the transactions into interplanetary file system (IPFS)-based off-chain storage system and the returned cryptographic hash into a blockchain ledger. In addition, we present a few issues and challenges that, in our

Motivated by the aforementioned challenges, this article discusses potential attack surfaces on IoT-enabled ZTNs systems, as well as recommended practices for dealing with those challenges using blockchain and DL.

Application	Area	Technology	Advantage	Limitation
Data security [2]	ZTNs	DL	Impact of AI on ZTNs	Limited evaluation
Security [3]	ZTNs	ML	Various use cases of ML in ZTNs	No ML-based case study presented
Security and trust [5]	ZTNs	Blockchain and AI	Various conceptual use cases in ZTNs	Lacks implementation
Diagnosis of faulty n/w links [9]	ZTNs	ML	Various prototypes and use cases in ZTNs	Low performance
Data security [8]	ZTNs	Blockchain	Improved security	High consensus computation cost
Network security [11]	NA	DL	Enhanced security	Low performance
Secure communication [12]	ITS	Blockchain	Reduced training time	High computational time

TABLE 1. A comparison of existing ZTN solutions.

The perception layer is also known as the hardware layer. It consists of various resource constrained sensors and actuators that send and receive data via different communication technologies such as Bluetooth, RFID, and 6LowPAN.

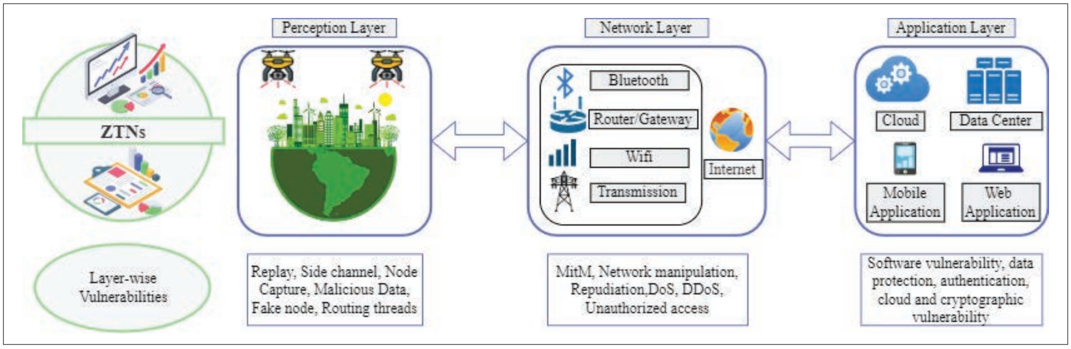
Perception Layer
Network Layer
Application Layer
ZTNs
Bluetooth
Router/Gateway
Wifi
Transmission
Internet
Cloud
Data Center
Mobile Application
Web Application
Layer-wise Vulnerabilities
Replay, Side channel, Node Capture, Malicious Data, Fake node, Routing threads
MitM, Network manipulation, Repudiation,DoS, DDoS, Unauthorized access
Software vulnerability, data protection, authentication, cloud and cryptographic vulnerability

FIGURE 2. Possible attacks and threats in IoT-enabled ZTNs.

opinion, can serve as a source of inspiration for upcoming research.

The rest of the article is organized as follows. In the next section, various attacks on different layers of IoT-enabled ZTNs are highlighted. Then we propose a novel secure data sharing mechanism consisting of a network and possible attack scenarios, and propose a blockchain and DL-based possible solution. We then highlight a few important open challenges for future directions in employing blockchain and DL for ZTNs. Finally, the article concludes in the final section.

Attack Surface on IoT-Enabled ZTNs

In this section, we discuss and highlight the possible attacks and threats on different layers of IoT-enabled ZTNs. Figure 2 shows the layered architecture and the associated attacks in each layer of an IoT-enabled ZTN ecosystem.

Perception Layer Attacks

The perception layer is also known as the hardware layer. It consists of various resource-constrained sensors and actuators that send and receive data via different communication technologies such as Bluetooth, RFID, and 6LowPAN. As these devices are often placed at different geographical locations, the possibility of node capture via physical access or fake node injection is high [7]. Moreover, they are also vulnerable to replay, side channel, malicious data, and routing thread attacks.

Network Layer Attacks

The network layer guarantees that data/information is routed and transmitted effectively. It uses WiFi, 3G, GSM, IPv6, and other communication protocols. While data/transactions are being exchanged, they may bring a variety of network vulnerabilities, including network manipulation (data transfer can be halted due to network floods or malicious gateway access), denial of service (DoS), distributed DoS (DDoS), man in the middle (MitM), unauthorized access, and a variety of connectivity vulnerabilities , including data integrity violations, poor quality of service (QoS), and so on.

Application Layer Attacks

The application layer, often known as the software layer, is the top layer that delivers business logic to systems and provides end users with user interfaces to support traffic management, mobility assessment, resource distribution, and forecast services. The application layer is mostly vulnerable to software flaws such as account enumeration, unsecured account credentials, and account suspension after a certain number of password guesses. Viruses, trojan horses, worms, and other malware can target cloud applications [5].

Case Study and Core Component of Deep Learning and Blockchain for Secure Data Sharing in ZTNs

In this section, we present a case study on a ZTN architecture to show how blockchain and DL can be used to enhance the data sharing mechanism. We exploit DL to design an IDS based on which the valid transactions are used by the smart contracts to run their consensus mechanism. Once the consensus is reached, the transactions are stored in IPFS ,and the returned hash is stored in a blockchain ledger. The core components of the proposed framework are explained below.

Network Model

The proposed framework for enabling secure data sharing in IoT-enabled ZTNs is shown in Fig. 3. It consists of four core components: the IoT network, edge servers, cloud server, and AI-enabled network manager. Each of these are explained below:

IoT Devices: This layer consists of various sensors and devices such as unmanned aerial vehicles, smartphones, smart meters, and temperature sensors. These devices are responsible for capturing and transmitting data to its associated access point (i.e., edge servers). This is due to the fact that most of these devices have limited computational power with limited storage. The fronthaul network acts as a communication medium between IoT and edge servers.

Edge Servers: This layer provides real-time analysis, visualization, and some local storage. The major requirement of IoT devices is real-time processing of sensory data. In such a scenario, the end user can use edge components to access data and run their latency-sensitive applications. Moreover, edge servers assist users in synchronizing cloud-directed data smoothly. These transactions can be forwarded to the cloud server for long-term storage via the backhaul network.

Cloud Servers: This layer mostly consists of several high-performance servers placed inside a data center that is managed by various service providers to offer limitless storage and computing capacity on demand. In ZTN applications, the cloud is primarily employed for in-depth, sophisticated analyses that do not require immediate attention.

The proposed approach uses edge servers in conjunction with the cloud server to improve resource usage and the quality of experience (QoE) of the services. However, these devices are assumed to be semi-trustworthy entities. Therefore, in order to

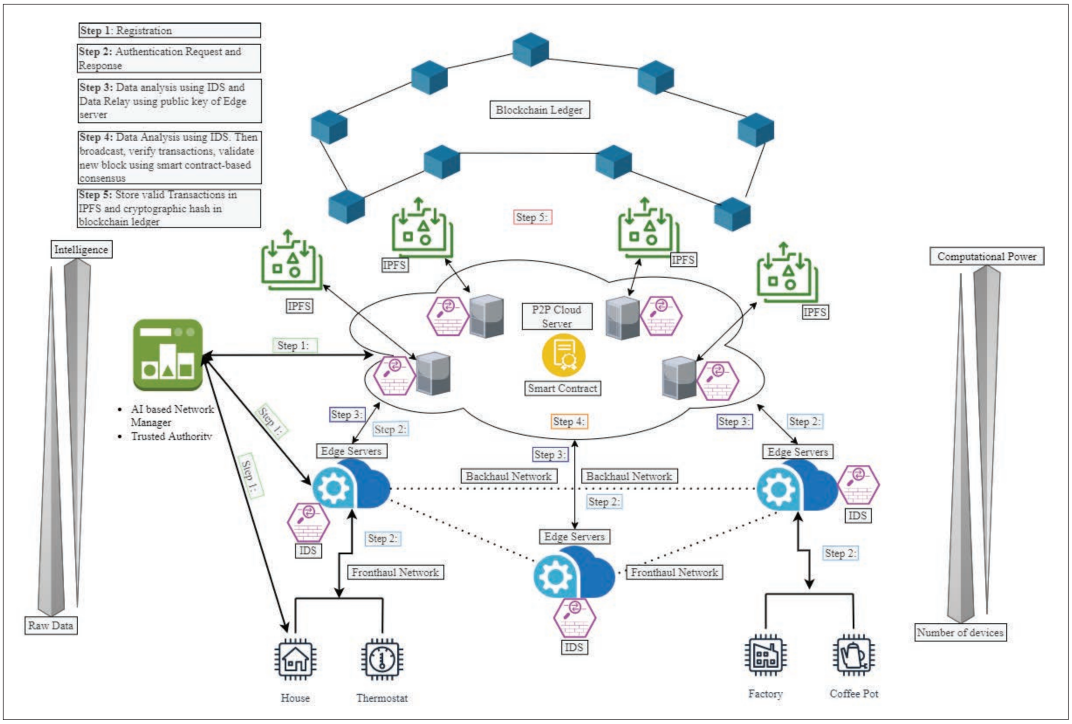

FIGURE 3. Proposed blockchain-based deep learning framework for secure data sharing in ZTNs.

The VAE is used to extract the features automatically, thus eliminating the need for domain-specific knowledge. Moreover, it is trained in an unsupervised manner to automatically extract features. The extracted features are then used by the AGRU technique to detect intrusion.

establish secure communication, all entities are initially registered and assigned credentials, including secret keys, by a trusted registration authority. After successful registration and key assignment, the data is shared among all entities. It should be noted that, the proposed IDS is trained on cloud servers but deployed on both edge and cloud servers. Once the data reaches the cloud server, the proposed DL-based IDS is used to check the data behavior. The valid data is then transmitted to smart contracts for mining using the efficient consensus algorithm. Once data is validated, the data is stored on an IPFS storage system, and the returned cryptographic hash is used to form the block. Thus, the proposed approach makes blockchain more efficient and lightweight for accessing data from cloud servers. The AI-enabled network manager automates monitoring, deployment, service provisioning, and network maintenance in the ZTN ecosystem.

Threat Model

In this article, we follow the Dolev–Yao (DY) model and the Canetti and Krawczyk (CK-adversary) model. An attacker can insert, modify, or delete the actual content of a message by eavesdropping on the communicated messages among participating entities. In this system, the IoT devices are not treated as trustworthy entities, while edge and cloud servers are assumed to be semi-trustworthy entities. We also assume that IoT devices can be physically captured by an attacker as it cannot be monitored 24/7, and therefore there is a possibility of direct physical capture of these devices. Under the current de facto CK-adversary model, an attacker can also compromise secret keys, credentials, and even session states during communication.

Proposed Secure Data Sharing Mechanism

This subsection presents the functioning of the proposed framework. It consists of two schemes:
1. A DL-based intrusion detection scheme
2. Blockchain and smart contract scheme

Below, we discuss the details of each scheme working separately.

DL-Based Intrusion Detection Scheme: An IDS is designed using a DL-based approach that combines a VAE with AGRUs (VAE-AGRU) for feature extraction and intrusion detection.

The VAE is used to extract the features automatically, thus eliminating the need for domain-specific knowledge. Moreover, it is trained in an unsupervised manner to automatically extract features. The extracted features are then used by the AGRUS to detect intrusion. RNN architectures are more commonly used for sequence prediction problems, but they suffer from vanishing gradients. The long short-term memory (LSTM) and GRU architectures solve the aforementioned problem and improve long-term dependency learning. Moreover, due to its twogated structure, which requires fewer parameters and hence less time to train and generalize, we utilize, GRU over LSTM for designing the proposed IDS [11]. We combine an attention mechanism with a traditional GRU, since assigning equal weights to spatial and temporal features can hamper the overall intrusion detection process. Therefore, the proposed VAE-AGRU IDS assigns more weights to discriminative spatial and temporal features.

Due to a real-time lack of IoT-based ZTN datasets, this article uses two real-world IoT datasets under a multi-classification problem setting. Initially, a data pre-processing step is used that follows two steps: label encoding and min-max normalization. In label encoding, all categorical values were converted into numeric values. Then we used min-max normalization to normalize each value of the dataset between 0 and 1, thereby preventing large values from adversely affecting the training process. The obtained dataset was divided into 70 percent training, and 30 percent testing sets. The proposed IDS monitors the incoming traffic at edge and cloud servers to filter the data or transactions into normal and attack types. It should be noted that we have not created a validation set while splitting the dataset using the *train_test_split* function of the *scikit learn* library. We instead used the *validation_split* parameter of the keras DL library. Moreover, cross-validation is often not used with DL models due to its greater computational expense. The normal transaction is forwarded to the blockchain and smart contracts scheme for further processing. Moreover, for attack instances, a log file is maintained based on which necessary action is taken by administration on the corresponding gateway and devices.

The transaction verification phase includes verification of meeting policies agreed upon by peers using smart contract execution over the edge and cloud severs. The transactions are taken as input using SC and verified by executing SC operations such as signature verification, timestamp, and public key verification.

Blockchain and Smart Contract Scheme: As illustrated in Fig.3, the blockchain and smart contract scheme consists of two major modules:

1. *IoT sensors registration and credential assignment*
2. *Transaction verification and storage*

The working of both modules is described below.

IoT sensors registration and credential assignment: The first module is responsible for registration of IoT sensors devices, where each sensor is assigned private and public keys. The entire process of registration and keys creation is performed by the trusted third party. The process broadcasts multiple public keys among the sensor nodes to enable secure communications. The signature of individual sensors is created using ECC, as ECC-based signatures are smaller and faster to produce certificates and public keys that are held by sensors and are more secure as well. The verification of individual sensors becomes easy, secure, and fast at higher key strengths using ECC-based certificates. While communication in ZTN sensors uses these keys for encryption and decryption, signature is being used for identity verifications. The digitally signed transaction is shared in the ZTN to ensure non-repudiation. Thus, the ZTN framework assures secure sharing of transactions and excludes public key infrastructure (PKI)-based certificate generation which mostly depends on third parties.

Transaction verification and storage: This module is responsible for transaction verification and storage. After successful registration of IoT sensors, the sensors can submit the transactions over the ZTN, as illustrated in Fig. 3. The transactions include several parameters including IoT sensor identity, timestamp, and access permissions such as store, read, and update. These access permissions are performed over an IPFS-based secure and distributed storage layer. The access permissions are mapped to an IPFS distributed hash table (DHT). Before granting of access permissions, the credential of IoT sensors nodes are verified like the public key of associated identity to ensure the transactions coming from verified sensors. However, six different phases need to be executed in ZTNs for successful verification and storage of transactions, namely transaction propose, transaction approve, transaction verify, transaction packing, transaction commit, and transaction store. In the transaction propose phase, IoT sensors initiate the registration process over the ZTNs and construct encrypted transactions using private keys and uses smart contracts (SCs) through application programming interfaces (APIs). The transactions approve phase includes authentication of identity and checking whether data is coming from a valid source or not.

The transaction verification phase includes verification of meeting policies agreed upon by peers using SC execution over the edge and cloud servers. The transactions are taken as input using SC and verified by executing SC operations such as signature verification, timestamp, and public key verification. The returned response gets recorded after successful verification, and then access permissions (create, read, update, and delete) are granted accordingly. For unsuccessful verification, access permission gets terminated by SC. The transaction packing phase includes a PoA consensus mechanism to aggregate the consent of peers and transactions dissemination over ZTNs. Next, the transaction commit phase includes validation of each transaction of block using SC execution, after which desired new blocks are committed to the ledger. Further, the store phase broadcasts the ledger across the blockchain network for ensuring synchronization among peers with the latest version of the ledger. Finally, the data are placed in two different storage units such as off-chain and on-chain storage through mapping data pointers. For off-chain storage, a DHT data repository of IPFS is used in ZTN. This ensures traceability and availability of data over the ZTN. DHT ensures self-organization and fault tolerace against false injection and routing attacks, and makes the framework more secure and robust.

Illustrative Results and Comparison

The experiments are performed on a Tyrone PC featuring an Intel® Xeon® Silver 4114 CPU @ 2.20 GHz (2 processors), 128 GB RAM, and a 2 TB hard disk. The Tensorflow library Keras is used to design the DL-based IDS. The implementation codes are executed using python programming language. The blockchain experiment is carried out on the Ethereum Ropsten Test network. The SCs are written in Solidity version (0.8.13). The experiments are performed on ToN-IoT and IoT-Botnet datasets; the dataset descriptions are mentioned in [14, 15]. The hyperparameters were selected based on random search of scikit-learn and keras libraries. This mechanism used batch size, epochs, learning rate, and optimization algorithm. We used a 2-layer VAE with 64 and 32 neurons, respectively, and a 4-layer AGRU architecture with 64, 32, 16, and 8 neurons, respectively. The DL model is trained with a batch size of 50 and an Adam optimizer. The training procedure used the cross-entropy loss functions. This article mainly focuses on multi-classification and therefore uses macro-averaging strategies to calculate accuracy (AC), detection rate (DR), precision (PR), F1 score, and false alarm rate (FAR) [2].

The proposed IDS based on VAE-AGRU model is trained with ToN-IoT and IoT-Botnet datasets. The numerical results and comparisons are shown in Table 2. It can be seen that the proposed approach has achieved 99.76 percent AC, 99.22 percent PR, 98.77 percent DR, and 99.10 percent F1 score, and has a reduced FAR of 0.0077 percent with the ToN-IoT dataset. Similarly, with the IoT-Botnet dataset, the proposed model has achieved 99.99 percent AC, 96.46 percent PR, 98.51 percent DR, and 97.28 percent F1 score, and has a reduced FAR of 0.0055 percent. The proposed approach has achieved high numerical values compared to the de Sousa *et al.* [9] and Benzaid *et al.* [2] models. The reason is that these models used flat features directly for training. Moreover, the attention mechanism on top of the proposed approach has helped in giving more attention to the spatio-temporal features that proved to

Authors	Year	Method	Dataset	Blockchain	AC	PR	DR	F1	FAR
de Sousa *et al.* [9]	2022	RF	ToN-IoT	No	97.81	87.55	85.43	86.41	1.21
			IoT-Botnet		97.47	78.40	76.62	77.45	5.52
de Sousa *et al.* [9]	2022	DT	ToN-IoT	No	95.34	74.42	80.00	76.33	7.14
			IoT-Botnet		96.92	78.31	77.85	77.99	7.88
Benzaid *et al.* [2]	2020	LSTM	ToN-IoT	No	98.62	97.68	97.70	96.43	1.11
			IoT-Botnet		98.44	97.41	96.88	95.41	1.01
Proposed model	2022	VAE-AGRU	ToN-IoT	Yes	99.76	99.22	98.77	99.10	0.0077
			IoT-Botnet		99.99	96.46	98.51	97.28	0.0055

AC: accuracy; PR: precision rate; DR: detection rate; FAR: false alarm rate.

TABLE 2. Quantitative comparison of performance with existing solutions.

The use of blockchain and DL-based IDS requires high computational power with large storage capabilities. In ZTN ecosystems, deployment, implementation, and training are complicated, and use resource consuming algorithms, such as consensus schemes and neural networks with large number of layers.

be more useful in identifying attacks. In the blockchain and SC scheme, Table 3 shows performance analysis using an SC policy and consensus mechanism applied over the ZTN. The different sets of transactions (Tx) are set up for 20 to 36 IoT nodes and successfully executed over the ZTN. The different matrices are calculated using blockchain-based analysis PoA such as Tx upload time, block mining time, and block creation time. The computational analysis depends on the number of IoT sensor registrations and number of Tx shared in the ZTN.

Even though the present work has achieved and proved to be effective, we have identified a few major challenges in applying DL and blockchain in the context of ZTNs. For example, the proposed approach has been tested and fixed to a maximum of 36 nodes with 304 Tx; however, in real-time applications, the number of nodes and Tx can gradually increase. For future work, it will be interesting to see how the proposed approach behaves in such environments, and we will try to overcome this limitation by designing a prototype. We have also listed and explained some other challenges of implementing DL and blockchain in the next section as potential directions for future research efforts.

Open Challenges and Future Research Directions in Employing Blockchain and Deep Learning for ZTNs

This section provides open challenges and future directions for the integration of blockchain and DL in current ZTNs.

Data Security Issues

In a ZTN ecosystem, IoT devices operate with low-quality software and default passwords, which makes them vulnerable to attackers. Thus, these devices open up various vulnerabilities in the network, and consequently, the communicating data can be exploited using software exploits, malware injection, failure of access control, and authentication schemes. Blockchain-enabled security solutions are also vulnerable to various data-security-related attacks such as credential leakage, impersonation, and data disclosure [1]. DL-based IDS has the capability to solve the above challenges to some extent. Nevertheless, applying DL-based IDS in real-time ZTN ecosystems is challenging due to the unverifiable or unknown data sources, as it can lead to erroneous or misleading results. Therefore, further research is needed to select suitable and reliable data sources.

Overall Complexity of the System

The adaptation of IoT devices and edge and cloud servers in ZTN ecosystems increases the complexity of the system. IoT devices have limitations in terms of computation and robust protection techniques. Moreover, edge and cloud servers are semi-trusted entities and require multilayer security controls in order to provide a robust security mechanism. The introduction of DL and blockchain makes these devices safe and secure, but also brings about complexities (e.g., computation and communication costs) in the system due to inherited properties [2]. Thus, system complexity is another major challenge and needs effective measures to handle it.

Computing Power

The use of blockchain and DL-based IDSs requires high computational power with large storage capabilities. In ZTN ecosystems, deployment, implementation, and training are complicated, and use resource consuming algorithms such as consensus schemes and neural networks with large numbers of layers. These costs can affect organizations with tight budget [3]. Therefore, there is a need for designing low-complexity efficient algorithms that require less computation power and storage capacity.

Scalability and Interoperability

The primary goal of applying ZTNs is automation. ZTNs not only help automate the network components, but also provide a way to alter the state of the deployed services. However, with the increase in users, IoT devices, the geographic, and distributed nature of the network increases the average transactions in the ecosystem. As a result, throughput does not expand as the network grows larger, and storing entire transactions on blockchain opens scalability issues. Therefore, due to limited storage and computational power, the number of transactions to be added in blockchain must be reduced.Various decentralized storage systems such as IPFS or Swarm can be used to solve scalability issues, but these platforms can be compromised as data are stored and available to the public [8, 10]. Moreover, current blockchain schemes face interoperability challenges due to the lack of standards and the diverse nature of consensus and blockchain platforms, which cre-

No of Tx	Transaction upload time over ZTN					Block mining time over ZTN					Block creation time over ZTN				
	20 nodes	24 nodes	28 nodes	32 nodes	36 nodes	20 nodes	24 nodes	28 nodes	32 nodes	36 nodes	20 nodes	24 nodes	28 nodes	32 nodes	36 nodes
38 Tx	0.70	0.83	0.82	0.74	0.60	11.38	15.83	17.95	18.04	23.82	9.48	13.92	15.06	15.24	19.11
76 Tx	0.73	0.92	1.04	1.32	1.41	18.08	22.43	24.71	23.20	33.84	16.18	20.54	21.83	25.32	29.16
152 Tx	0.74	1.11	1.41	1.47	1.53	32.09	38.49	41.06	44.55	72.84	24.18	35.63	43.17	49.77	64.20
304 Tx	1.12	1.36	1.50	1.51	1.72	65.30	72.19	82.09	85.62	143.72	39.41	50.35	57.31	71.84	93.15

TABLE 2. Blockchain-based analysis over ZTNs.

ate significant communication limitations. In this direction, various compression algorithms with high compression ratios and lightweight designs should be developed to reduce the cost of large-scale deployment of DL and blockchain services.

Real-World ZTNs and Dedicated Datasets

The ZTN ecosystem is in its infancy and requires real-world ZTN dedicated datasets to exploit its full potential capabilities. The availability of real-world datasets will help researchers to design efficient and effective IDSs for ZTNs [9]. Moreover, the availability of datasets enables researchers to build a benchmark for training, validating, and evaluating experiments with different DL techniques.

Conclusion

This article introduces the next-generation network infrastructure of ZTNs and their integration with IoT. We cover a number of related studies, as well as their drawbacks, that attempted to use deep learning and blockchain to address the secure data sharing challenge encountered with ZTNs. We highlight the major attack and threat vectors of IoT-enabled ZTNs that can hinder the realization and goal of automation. As a case study, we designed a secure data sharing framework using deep learning and blockchain technology. The main goal of this scheme was to first differentiate normal transactions from abnormal ones. Then the valid transactions were used by smart contracts to run consensus mechanisms. Once the consensus was reached, the transactions were stored in an interi-planetary file system, and the returned hash was stored in blockchain, making the ledger lighter. Finally, we discuss future research directions in using blockchain and deep learning for ZTNs, urging additional researchers to contribute in this direction.

References

[1] I. Al Ridhawi and S. Otoum, "Supporting Next-Generation Network Management with Intelligent Moving Devices," *IEEE Network*, vol. 36, no. 3, May.June 2022, pp. 8–15.

[2] M. Aloqaily *et al.*, "Realizing the Tactile Internet Through Intelligent Zero Touch Networks," *IEEE Network*, 2022.

[3] J. Gallego-Madrid *et al.*, "Machine Learning-Based Zero-Touch Network and Service Management: A Survey," *Digital Commun. and Networks*, vol. 8, no. 2, 2022, pp. 105–23.

[4] M. W. Akhtar and S. A. Hassan, "Tantin: Terrestrial and Non-Terrestrial Integrated Networks-A Collaborative Technologies Perspective for Beyond 5G and 6G," *Internet Technology Letters*, 2021, p. e274.

[5] G. Carrozzo *et al.*, "AI-Driven Zero-Touch Operations, Security and Trust in Multi-Operator 5G Networks: A Conceptual Architecture," *2020 Euro. Conf. Networks and Commun.*, 2020, pp. 254–58.

[6] Z.-T. Network, "Service Management (ZSM)," Ref. Architecture, ETSI GS ZSM, vol. 2, 2020, p. V1.

[7] C. Grasso, R. Raftopoulos, and G. Schembra, "Smart Zero-Touch Management of UAV-Based Edge Network," *IEEE Trans. Network and Service Management*, 2022.

[8] K. U. Nisa *et al.*, "Security Provision for Protecting Intelligent Sensors and Zero Touch Devices by Using Blockchain Method for the Smart Cities," *Microprocessors and Microsystems*, vol. 90, 2022, p. 104,503.

[9] N. F. S. de Sousa *et al.*, "Machine Learning-Assisted Closed-Control Loops for Beyond 5G Multi-Domain Zero-Touch Networks," *J. Network and Systems Management*, vol. 30, no. 3, 2022, pp. 1–29.

[10] P. K. Sharma *et al.*, "Distblocknet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Commun. Mag.*, vol. 55, no. 9, Sept. 2017, pp. 78–85.

[11] M. S. Ansari, V. Bartôs, and B. Lee, "Gru-Based Deep Learning Approach for Network Intrusion Alert Prediction," *Future Generation Computer Systems*, vol. 128, 2022, pp. 235–47.

[12] M. Wazid *et al.*, "Fortifying Smart Transportation Security Through Public Blockchain," *IEEE IoT J.*, vol. 9, no. 17, 2022, pp. 16,532–45.

[13] B. Bera *et al.*, "Private Blockchain-Based AI-Envisioned Home Monitoring Framework in IoMT-Enabled Covid-19 Environment," *IEEE Consumer Electronics Mag.*, 2021.

[14] N. Moustafa, "Ton IoT Datasets," 2019; http://dx.doi.org/10.21227/fesz-dm97, accessed 10 Feb. 2020.

[15] Ullah and Q. H. Mahmoud, "IoT Botnet Datasets," 2020; https://sites.google.com/ view/iotbotnetdatset, accessed 5 Apr. -2020.

Biographies

Randhir Kumar [M] (randhir.honeywell@ieee.org) received his Ph.D. degree in information technology from the, National Institute of Technology Raipur, India, in 2021. He is currently working as an assistant professor with the Department of Computer Science and Engineering, SRM University AP, India. Before joining SRM University, he worked as a postdoctoral researcher with the Department of Electrical Engineering, Indian Institute of Technology Hyderabad. He has published more than 40 research articles in reputed journals and conferences. His research interests include cryptographic techniques, information security, blockchain technology, and web mining.

Prabhat Kumar [M] (prabhat.kumar@lut.fi) received his Ph.D. degree in information technology from the, National Institute of Technology Raipur under the prestigious fellowship of the Ministry of Human Resource and Development (MHRD) funded by the Government of India in 2022. He is currently working as a postdoctoral researcher with the Department of Software Engineering, LUT University, Lappeenranta, Finland. He has many research contributions in the areas of machine learning, deep learning, federated learning, big data analytics, cybersecurity, blockchain, cloud computing, the Internet of Things, and software defined networking.

Moayad Aloqaily (moayad.aloqaily@mbzuai.ac.ae) received his Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ontario, Canada, in 2016. He was an Instructor with the SYSC Department, Carleton University, Ottawa, in 2017. From 2018 to 2019, he was an assistant pProfessor at the American University of the Middle East (AUM), Kuwait. From 2019 to 2021, he was the cybersecurity program director and an assistant professor with the Faculty of Engineering, Al Ain University, UAE. He has been the managing director of xAnalytics Inc., Ottawa, since 2019. He is currently with the Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE. His current research interests include applications of AI and ML, connected and autonomous vehicles, blockchain solutions, and sustainable energy and data management.

Ahamed Aljuhani (A_aljuhani@ut.edu.sa) received his M.S. degree in computer science from the University of Colorado Denver and his Ph.D. degree in computer science/information security track from The Catholic University of America, Washington, DC. He is currently an assistant professor and the chair of the Department of Computer Engineering, College of Computing and Information Technology, University of Tabuk, Saudi Arabia. His current research interests include information security, network security and privacy, secure system design, and system development.