International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 19 Issue 02, FEB, 2019

BLOCKCHAIN AND IOT INTEGRATION: ENHANCING SECURITY PERSPECTIVES

[#1]**Mr.N SANTHOSH KUMAR,** *Assistant Professor*

[#2]**Mr.CHADA SAMPATH REDDY,** *Assistant Professor*

Department of Computer Science and Engineering,

SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Blockchain (BC), a Bitcoin cryptocurrency spinoff, has gained considerable attention due to its usefulness in a range of disciplines, particularly complicated non-monetary systems. A Blockchain-based distributed ledger can be made exceedingly safe and immutable by combining cryptographic techniques such as hashing and asymmetric encryption with a distributed consensus approach. This removes the need for any intermediaries. On the other hand, the network is being flooded with Internet of Things (IoT) devices. This event is more dangerous in terms of privacy and safety. As a result, addressing the security problems generated by the growing IoT ecosystem is critical. This study looks into how BC can be used to improve IoT security and privacy. Recent research articles and projects/applications were surveyed in order to evaluate BC for IoT Security deployment, identify relevant difficulties, and give solutions for BC-enabled increased security for the IoT ecosystem.

Keywords:Blockchain, Blockchain of Things (BCoT), Distributed Ledger Technology (DLT), Internet of Things(IoT), Proof-of-Work (PoW), Security

1. INTRODUCTION

This article covers the future of Blockchain of Things (BCoT) integration and how Blockchain technology could improve IoT ecosystem security. Blockchain technology is innovative, but this study summarizes research over the past decade. This research examines how Blockchain could improve IoT security. Blockchain and other digital ledger technologies' applications, limitations, privacy, and security issues are examined to attain this goal. This paper presents our findings from London Metropolitan University's 2018 International Conference on Emerging Technologies in Computing.As with other computing businesses, the IoT ecosystem promotes security and privacy. Blockchain is considered essential for IoT security and privacy, improving its foundation. Blockchain scholars and industry professionals are exploring new uses and perspectives.Regular exercise is common. Proof-of-Work (PoW) solves math problems. By keeping a complete digital database of all transactions, the blockchain maintains its integrity. These transactions are final. Figure 1 shows a high-level BC technology schematic system block diagram. This study examines social media's mental health consequences.

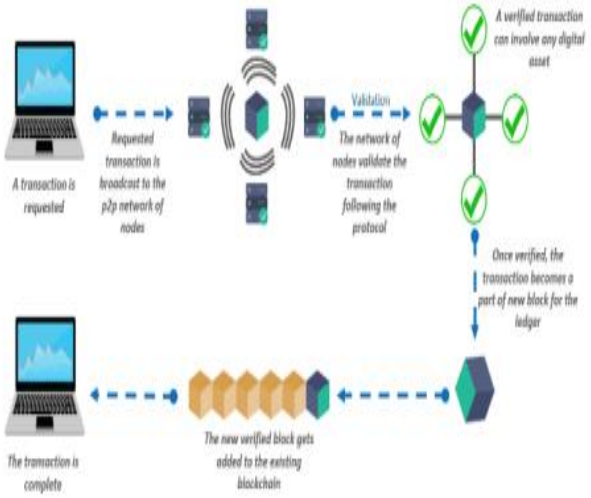

Figure 1. Blockchain concept overview.

The purposely unpredictable Public Key in Blockchain technology offers maximum security while registering user identities. So, more privacy is assured. Blockchain technology has been successful in non-financial applications in several studies and project reports. Supply chain management, healthcare systems, online and

electronic voting, location verification, distributed cloud storage, securities settlement, and HR management and recruitment are examples. Figure shows six-tiered hierarchical blockchain design. The second point, "2," is below.

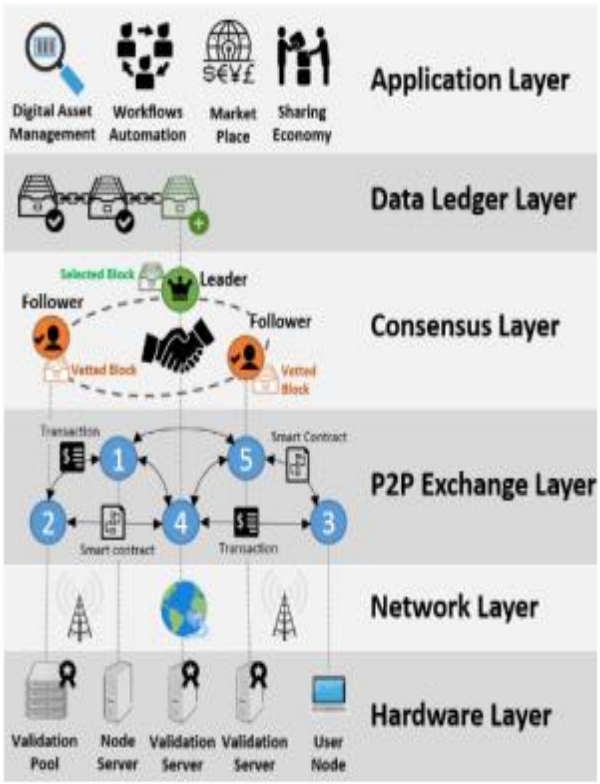

Figure 2. Blockchain Technology Layer Model

This study examined academic literature and related projects/applications to assess if Blockchain may improve IoT security. They also identified Blockchain deployment problems in this business and suggested Blockchain-based IoT security system improvements. Examines IoT, IoE, WSN, and DLT knowledge domains, focusing on Blockchain and crypto-currency.

2.BLOCKCHAIN FUNDAMENTALS

Understanding how Blockchain works is essential to understanding how it could improve IoT security. After this brief overview of Blockchain, the next session covers the IoT ecosystem.

Two interdependent parts make up a Blockchain. These items:

Transaction: In blockchain-like digital ledgers, participants start transactions.

Block: Blockchain blocks store transactions and other data like event order and creation time.

Blockchains are private or public depending on their use. Most public blockchains allow everyone to read and write. Bitcoin production and circulation documentation is public Blockchain. Some public Blockchains restrict write and read access, depending on their function. A private Blockchain hides users' identity. Access is restricted to trustworthy participants or a single organization. A "consortium blockchain." Government agencies and subsidiaries need blockchain technology. Due to its public nature, blockchain technology is secure and open. Each network node has its own blockchain with updated records and transactions, ensuring data integrity. Public can verify unlawful or unexpected changes. These public blocks are hashed and encrypted using a private key for security and anonymity. Data encrypted with the private key is unreadable.

Blockchain can be applied centrally, however decentralization is its main feature. It's decentralized because:

Blockchain network nodes store transactions and blocks instead of a single node.

Rules or algorithms verify transactions, reducing bias from a single authority. This approach requires a lot of trust to get consensus.

Only validated blocks can be added to blockchains. Since previously attached blocks are public and widely distributed, they are transparent and easy to verify, making them immutable. Blockchain ecosystems outperform other technologies due to their full security.Transactions are not immediately added to the blockchain, a network of nodes. An started transaction must be confirmed and verified before joining the chain. To function properly, blockchain nodes must follow rules or algorithms. Different algorithms define what is "valid" in Blockchain. Multiple transactions per block are common. All Blockchain nodes receive the new block to add to their chains. Next block in chain contains previous block's hash, or digital trace.

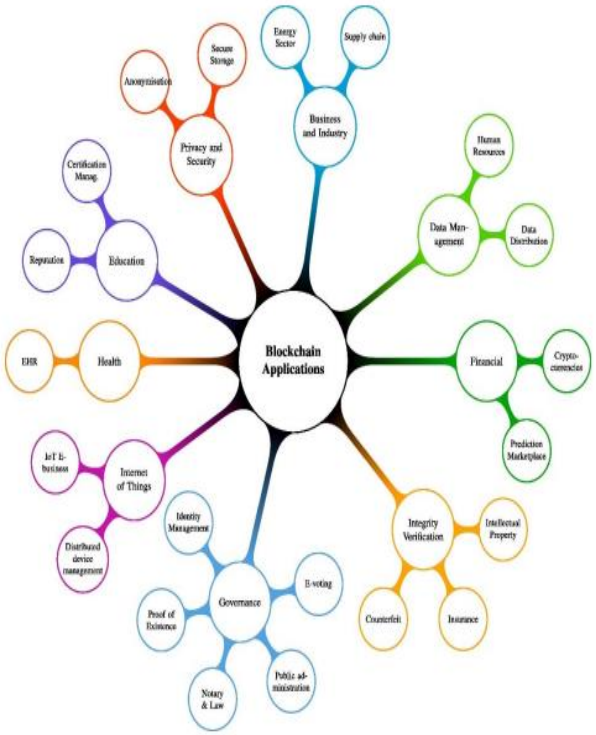

Figure 3. A typical blockchain implementation

The Blockchain verifies and stores new transactions permanently. User or participant identity data is also protected. During transaction verification, user data is protected. To reconcile widespread cooperation, a computer-coded digital ledger records all transactions. Instead of mutual trust or an intermediary, blockchain members must trust the decentralized network structure. Blockchain means "Trust Machine".

Early Blockchain adopter Bitcoin is one example. Blockchain technology has several uses in healthcare, HR, recruitment, maintaining and authenticating legal documents like deeds and certificates, IoT, and the Cloud. As Tapscott (year) correctly mentioned, Blockchain is a "World Wide Ledger" with creative uses beyond transaction verification. Decentralized groups, recorded wisdom, and independent government services are examples. The figure. This article discusses traditional and novel blockchain applications.Figure 1 shows blockchain use. The fourth example shows biological applications' diversity. The figure. The paper also lists six further reasons to use blockchain technology: access control, non-repudiation, data versioning, integrity, auditing, and provenance.

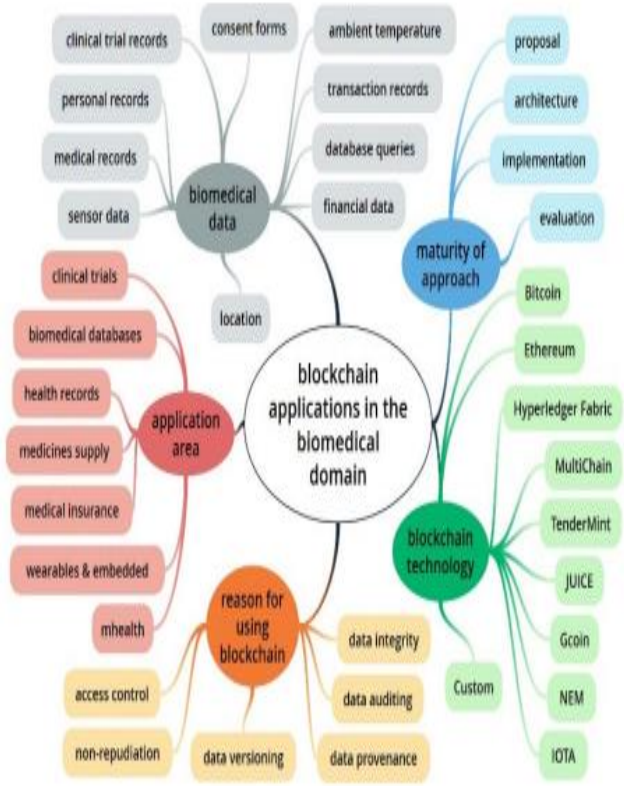

Figure 4. Blockchain visualization in biomedicine.

INTERNET OF THINGS (IOT)

The 'Internet of Objects' or 'Internet of Things' ('IoT') connects electronic and electrical devices of various sizes and purposes to the Internet. This link is made mostly using wireless sensors, except for the Internet. IoT devices are often introduced, expanding connections beyond machine-to-machine.IoT devices span various protocols, applications, and networks. Short-range wireless technologies including sensor networks, RFID, ZigBee, and location-based technologies are connecting physical items to the Internet, advancing IoT technology.

The Internet Business Solutions Group (IBSG) recognized IoT as a distinct entity when more inanimate things were directly connected to the Internet without human intermediaries. From CISCO's 'Planetary Skin' to the Smart Grid and intelligent automobile IoT, acceleration has increased. This tendency will make the Internet widespread as gadgets are integrated into consumer appliances, including personal and intimate goods used daily. Internet of Things (IoT) devices solely use Internet networking

protocols, not Internet or peer interfaces. This limitation needs rapid attention.

The Internet of Things (IoT) can improve privacy, security, and administration by connecting car electronics, home environmental management systems, telephone networks, and domestic utility service control mechanisms. The IoT's expanding range and network integration are shown. Five components make up a typical IoT ecosystem:

Sensors: Data collecting and conversion require sensors.

Computing Node: Processing sensor data requires CPU-powered nodes.

Receiver: A transceiver receives communications from local and remote computing nodes or other linked devices.

Actuator: The Computing Node may choose an electro-mechanical actuator. The attached gadget starts after processing sensor and Internet data.

Device: It executes a task when activated.

2. BC ENABLED ENHANCED IOT SECURITY

In an IoT environment, M2M communication dominates without human involvement. IoT hasn't solved machine trust. Blockchain improves scalability, security, reliability, and privacy. Blockchain can track the massive number of IoT devices and coordinate transaction processing. Indeed, "Shodan," "the inaugural search engine designed for Internet-connected devices," will identify insecure IoT devices, underlining their need for repair. Blockchain removes Single Points of Failure in IoT ecosystems, enhancing reliability. Blockchain encrypts data with cryptographic methods and hashing. Blockchain technology in IoT may improve security. IoT devices cannot compute hashing or cryptographic methods. This constraint demands more research, including extending the in situ powering source's longevity.Underwood thinks Blockchain might transform the digital economy. Blockchain technology prioritizes trust. Blockchain can collect chronological and sequential transaction data as a massive networked time-stamping mechanism. NASDAQ records confidential securities transactions using its 'Linq blockchain' system. Financial resolution for post-trade concerns and swaps is offered by Axoni and DTCC. Regulators like British Columbia's safe, discreet, and traceable real-time transaction monitoring.We must prioritize operational technology security. Industrial IoT and OT devices can be managed and secured using blockchain to prevent data modification and spoofing. After successful deployment and operation, the blockchain records compromised sensors, devices, and controllers, making them tamper-resistant.

Wireless sensor network (WSN) technology renders IoT privacy and security susceptible. Due to its design, architectural consensus method, and cryptographic tools, Blockchain is a Trust Machine. Many IoT security vulnerabilities can be reduced. Miraz thinks blockchain and IoT can collaborate. BC needs participating nodes for agreement; IoT can help. BC can secure IoT. Example: transparency, privacy, immutability, operational resilience.

Internet of Things (IoT) creates a connected ecosystem by linking physical and information systems. Many issues have prevented IoT security from being properly considered in device and product design. IoT research has changed due to blockchain technology (BC). This transformation integrates IoT and BC for cyber resilience and safety. However, these technologies' underdevelopment causes several integration issues. Numerous studies recommend adopting blockchain technology to secure IoT ecosystems, especially against "Stalker" attacks.

The Internet of Things relies on wireless sensor networks. All IoT nodes are subject to attacks, including DDoS. Compromise could break these nodes. IoT networks are cloud-dependent. SPF makes centralized architecture more vulnerable.

IoT devices send lots of data online for processing and decision-making. In the IoT ecosystem, data privacy and secure authentication are key challenges. Massive data sets can be misused without protection. Thus, safeguarding the IoT system from injection attacks and spoofing is

critical. Injection attacks manipulate system decisions by inserting bogus data or measures.

Data-generating sensors can share and sell data across autonomous systems and marketplaces in the Machine Economy. However, trusting parties remains difficult. Non-repudiation can be addressed with a publicly verifiable audit-trail system without a third party. Piloted blockchain apps include FileCoins and Trans Active Grids. These apps let devices trade and make money.

Splits data before delivering it to IoT-enabled smart home devices using pseudonymization. The blockchain (BC) certifies IoT device data and keeps cryptographic hashes. Public keys are used by the owner to reconstruct data and create access procedures for smart devices and service providers. Figure 1 displays BC layers in the framework. 2, eliminating security concerns in the application, database, communication, and physical layers. Ethereum smart contracts leverage blockchain as a distributed database. The BC (Blockchain) application layer secures dependent operations from unauthorized access.

Filament integrates blockchain with Telehash2. Filament's blockchain-smart contract prototype connects smart IoT devices. This allows devices interact, discover, and function independently. Devices must authenticate before communicating. These authentication methods use TLS and SSL, which require public key infrastructure. Prabhu et al. [year] took a different technique than [authors]. Blockchain technology allowed the IoT ecosystem to access data on the decentralized ledger utilizing IP addresses. The system notifies via ledger events.

In an IoT ecosystem, intermediary devices may hop. Thus, a secure architecture that respects private communication protocols is necessary. The Berlin firm Moeco created the Moeco prototype for secure IoT smart device connectivity. Moeco builds the "Domain Name System (DNS) of things" for IoT data routing using blockchain. Moeco uses Ethereum, but future research may integrate Exonum, a Byzantine consensus method .

Similar to their purpose, Hashemi et al. (year) suggest a publish-subscribe technique for IoT data security. This study has two objectives:

Distinguish data storage from administration;

Design distributed, decentralized, scalable components.BC enhances transparency and durability in the three-layer prototype's Data Storage system. Data Management collects access-controlled data decentralized via blockchain-enabled role-based interactions. These interactions involve data source, owner, endorser, and requester.

One of the largest obstacles facing IoT data security is meeting the authentication and access control demands of the decentralized IoT ecosystem, which has devices with little computing power. ACLs, DACs, MACs, and ABACs are unsuited for IoT's decentralized design. Deters [43] suggests blockchain (BC) and smart contracts for this. For permanent recording, the data or resource owner must sign credentials and submit a "Announcement" transaction to the blockchain ecosystem. You must request data from a smart contract to obtain it.

Bahga and Madisetti created a new method for applying BPIIoT in Cloud-based Manufacturing (CBM) systems. This approach offers manufacturing resources and capabilities as a cloud service. Smart contracts and changing public keys secured Ethereum transactions. Supply chain-specific cloud computing, IoT, and BC integration requirements are examined by Korpela et al. In integrated digital supply chains, cloud computing and IoT can enable cost-effective business strategies. Digital supply networks can be transformed by blockchain technology (BC).Industry 4.0 could employ blockchain-enabled IoT devices for smart energy exchange. Blockchain technology is designed for M2M communication, making this important. Smart gadgets can trade steam and natural gas using blockchain technology. Energy producers post pricing via blockchain transactions, and consumers use bitcoin to get the best offer.

Dorri et al. (year) created a multitier blockchain for privacy and security. This design meets IoT requirements while minimizing blockchain

consensus mechanism limits. BC's computationally intensive Proof of Work (PoW) consensus process opposes green computing. One miner manages an access policy-based strategy. It employs cloud storage and an overlay network. Miners create blocks for new nodes, like smart devices. This header connects to the previous block in the chain, whereas the other accommodates data access policy. Blockchain (BC) applications use symmetric keys, such as the Diffie-Hellman algorithm, to improve node communication privacy and secrecy. Miners manage and distribute keys. The miner becomes a central authority, reducing blockchain's decentralization.BC integration secures IoT, and smart contracts enable new business models and problem-solving. But smart contract vulnerabilities must be considered. Wörner et al. (year) exchange sensor data using Bitcoin. Each network sensor node's address is Bitcoin public key. Bitcoin transfers to sensors are needed to get data. The sensor responds to the node with the appropriate data after verification. This generalizes Zhang and Wen's IoT electric business model.The peer-to-peer (P2P) Enigma framework lets many participants store and process data in complete secrecy, according to Zyskind et al. The purpose is to safely spread data among several nodes while isolating it from its references, making data reconstruction harder. A Distributed Hash Table (DHT) for shared secret data pieces and an external Blockchain (BC) system for access control, network monitoring, and identity management help achieve this goal. Shafagh et al. created a BC-enabled auditable IoT data storage system similarly.

IOTA, an open-source cryptocurrency developed by the group, enables micro-payments for the Internet of Things. TANGLE is IOTA's breakthrough blockchain technology. TANGLE scales better than block-and-miner blockchains because of acyclic graphs.

Chakraborty et al. developed a level 0 and level N IoT security architecture. Resource-constrained nodes are handled by this framework. Security primitives for Level 0 devices are computationally constrained. In contrast, level N has major and subsidiary nodes. Data processing, communication, access control, and more happen in primary nodes. However, minor nodes aid primary nodes. Level 0 nodes cannot connect directly due to resource limits. Intermediate nodes at level N can implement secure indirect connections.

3. CONCLUSION

To answer "To what degree can the utilization of Blockchain technology enhance the overall security of Internet of Things (IoT) ecosystems?" this article introduces these two evolving technologies' operational procedures. We also covered IoT security. The study then examined whether Blockchain might secure IoT ecosystems.

Blockchain and IoT have various uses and are promising. Beyond Bitcoin manufacturing and transactions, blockchain has proven its value in safe networked transactions. The Internet of Things (IoT) has expanded beyond wireless sensor networks. Privacy, security, traceability, data provenance, and precise time-stamping are improved by blockchain. These powers exceed prior technology. Blockchain secures H2H, M2M, and H2M transactions. Blockchain technology is reliable, especially with the rise of IoT. This decentralized application in the global Internet architecture promotes network redundancy, data redundancy through dispersion, and survivability.

REFERENCES

1. Mahdi H. Miraz and Maaruf Ali, “Blockchain Enabled Enhanced IoT Ecosystem Security”, Proc. of the Int. Conf. on Emerging Technologies in Computing 2018 (iCETiC ‘18), Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, London, UK, 2018, pp. 38-46. Available: https://link.springer.com/chapter/10.1007/978-3-319-95450-9_3.
2. Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Safeeullah Soomro, Mohammad Riyaz Belgaum, Mahdi H. Miraz, Jawdat Alshaer, “Challenges of

Internet of Things and Big Data Integration", Proc. of the Int. Conf. on Emerging Technologies in Computing 2018 (iCETiC '18), Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications UK, 2018, pp. 47-55. Available: https://link.springer.com/chapter/10.1007/978-3-319-95450-9_4.

3. Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Mohammad Riyaz Belgaum, Jawdat Alshaer, Safeeullah Soomro, Mahdi H. Miraz, "Internet of Things: Infrastructure, Architecture, Security and Privacy", 2018 Int. Conf. on Computing, Electronics & Communications Engineering (iCCECE), Southend, United Kingdom, 2018, pp. 150-155, doi: 10.1109/iCCECOME.2018.8658516.
4. Ameer Rosic, "Proof of Work vs Proof of Stake: Basic Mining Guide", Blog 2017. Available: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake.
5. Shashank, "Blockchain Technology – Unfolding the Technology behind Bitcoins", Blog 2017. Available: https://www.edureka.co/blog/blockchain-technology/.
6. Mahdi H. Miraz and David C. Donald, "Application of Blockchain in Booking and Registration Systems of Securities Exchanges", Proc. of the IEEE Int. Conf. on Computing, Electronics & Communications Engineering 2018 (IEEE iCCECE '18), Southend, United Kingdom, 16-17 August 2018, pp. 35-40, doi: 10.1109/iCCECOME.2018.8658726.
7. David C. Donald and Mahdi H. Miraz, "Multilateral Transparency for Securities Markets through DLT", in the Fordham Law Engineering (LNICST), vol. 200, London, Review, Vol. XXV, Issue 1, January 2020, pp. 97-153. Available: https://ir.lawnet.fordham.edu/jcfl/vol25/iss1/2/.
8. Md Mehedi Hassan Onik, Mahdi H. Miraz, and Chul-Soo Kim, "A Recruitment and Human Resource Management Technique Using Blockchain Technology for Industry 4.0", Proceeding of Smart Cities Symposium (SCS-2018), Manama, Bahrain, 2018, pp. 11-16. doi: 10.1049/cp.2018.1371.
9. Omar Dib, Kei-Leo Brousmiche, Antoine Durand, Eric Thea and Elyes Ben Hamida, "Consortium Blockchains: Overview, Applications and Challenges", International Journal on Advances in Telecommunications, vo1. no.1 & 2, 2018, p. 51-64. Available: http://www.iariajournals.org/telecommunications/tele_v11_n12_2018_paged.pdf.
10. Fran Casino, Thomas K. Dasaklis and Constantinos Patsakis, "A systematic literature review of blockchain- based applications: Current status, classification and open issues", Telematics and Informatics, vol. 36, March 2019, pp. 55-81, ISSN 0736-5853, doi: 10.1016/j.tele.2018.11.006, Elsevier Ltd. Available: http://www.sciencedirect.com/science/article/pii/S0736585318306324.