BCT-CS: Blockchain Technology Applications for Cyber Defense and Cybersecurity: A Survey and Solutions

Naresh Kshetri[1]*, Chandra Sekhar Bhushal[2], Purnendu Shekhar Pandey[3], Vasudha[4]
Assistant Professor (Cybersecurity), Dept. of Math, CS & IT, Lindenwood University, St. Charles, MO, USA[1]
School of Eng, IT & Physical Sciences, Federation University, Victoria, Australia[2]
Department of CSE, KIET Group of Institutions, Ghaziabad, UP, India[3]
Department of CSE, United Institute of Management, Prayagraj, UP, India[4]

***Abstract*—Blockchain technology has now emerged as a ground-breaking technology with possible solutions to applications from securing smart cities to e-voting systems. Although it started as a digital currency or cryptocurrency, bitcoin, there is no doubt that blockchain is influencing and will influence business and society more in the near future. We present a comprehensive survey of how blockchain technology is applied to provide security over the web and to counter ongoing threats as well as increasing cybercrimes and cyber-attacks. During the review, we also investigate how blockchain can affect cyber data and information over the web. Our contributions included the following: (i) summarizing the Blockchain architecture and models for cybersecurity (ii) classifying and discussing recent and relevant works for cyber countermeasures using blockchain (iii) analyzing the main challenges and obstacles of blockchain technology in response to cyber defense and cybersecurity and (iv) recommendations for improvement and future research on the integration of blockchain with cyber defense.**

***Keywords*—Applications; blockchain technology; blockchain solutions; countermeasures; cyber-attacks; cyber defense; cybersecurity; survey**

I. Introduction

Cyber defense is a defensive mechanism or coordinated act of resistance designed for the safety of information, system, and networks against offensive cyber operations by implementing various security procedures. Some of the major cyber defense activities include set up and maintenance of the hardware and software for security infrastructure, examination of the network's system for vulnerabilities, implementation of real-time countermeasures to stop zero-day attacks, and recovery from attacks that were either completely or partially successful [1]. It ensures the survival of any state from cyber-attacks [2]. The main focus of cyber defense is the prevention, detection, and regulation of timely response to cyber-attacks or threats to make sure that infrastructure or information are not harmed. Cyber defense aims to reduce possible attacks and understand the critical location and sensitive information by carrying out various technical analyses to find out the possible paths and areas that could be targeted by the online attackers [3].

To achieve regulatory compliance, protect assets, and compromise the assets of adversaries, information safeguards, security procedures, and IT security tools and techniques are governed, developed, managed, and applied in cybersecurity [3]. It is the actions and policies implemented to protect cyberspace by the military, public and private business sector. Cyber security has been identified as one of the crucial strategic fields of national security [4]. It is related to protecting information/data, infrastructure, and service to reduce the possibility of loss, damage, and compromise of misuse by unauthorized users. Mainly cyber security focuses on sensitive information stored electronically on computers, computer networks, mobile devices, and the internet [5].

Blockchain is a distributed database technology based on cryptography that maintains a constantly expanding list of data entries that are verified by every network node. Data records are stored in blocks, which are linked together to form the chain. Each participating node keeps a replica of the data records and transmits it to every other node in the network, improving trust and transparency, as opposed to information being routed through a central node [6]. Blockchain technology minimizes the probability of unsecured transactions because applications function decentralized and do not require intermediary authority to monitor the transactions between participants [7].

Blockchain underlying characteristics of decentralization, consensus mechanism, immutability, traceability, and privacy provide a strong foundation for cyber defense and security of data and information in cyberspace. Blockchain decentralized property with use of distributed ledger eliminates the intermediaries that are potential risk for security of the network. Also, there is no single point of failure in decentralization so there is a very low chance that an IP-based DDoS attack will disrupt the daily operations. By establishing a decentralized network using client-side encryption where data owners have complete transparency of their data, blockchain increases the security of data sharing and storing [8] [9]. Next blockchain's Consensus mechanisms govern how participants agree on a single common version of the facts when storing and verifying blocks (a shared truth). The Consensus enables nodes to trustworthily verify brand-new

*Corresponding Author.

blocks in the network. The Consensus enables nodes to trustworthily verify brand-new blocks in the network [9].

The immutability property of blockchain ledger provides the solid base for data integrity. Each transaction in a block is cryptographically signed by its sender, and every block in the blockchain is signed by its miner. To alter a single transaction in the blockchain, an attacker ought to modify each next block in the same manner, resolving the consensus problem for that block and all succeeding blocks, and convincing more than 50% of users on the network to adopt the updated chain. Modifying blocks in the network is nearly impossible due to the hashing features and the amount of computing and electrical effort required to achieve this goal [8] [9]. Traceability characteristics of blockchain technology makes the network more secure. Every transaction uploaded to the blockchain is digitally signed and timestamped, allowing organizations to go back to a precise time period for each transaction and identify the corresponding participant (by their public address) on the blockchain [8]. Privacy is one of the core properties of blockchain technology. The identity of those involved in a transaction is protected by cryptographic functions that ensure the anonymization of the entities participating in the blockchain, which help to gain a high degree of privacy [9].

The rest of the article is organized as related work in Section II which discusses several recent works of blockchain-based security and models. We then presented Section III of our paper as BCT for cyber defense and cybersecurity. Section IV of our study is about Countermeasures and defense initiatives with the help of blockchain technology. The advantages of blockchain technology with respect to cyber defense and cybersecurity are summarized in Section V of our findings. We have pointed out several solutions and challenges while incorporating those blockchain-based solutions in Section VI (blockchain-based solutions and challenges). In Section VII, we presented the conclusion and future scope of the study as recommendations for improvement and future research on the integration of blockchain with cyber defense.

II. Related Works

In [10], A. Razaque et al. (2021), introduced a web-based Blockchain-enabled cybersecurity awareness program (WBCA) to reduce the risk of cybercrimes. The proposed WBCA enhances user understanding of cybersecurity hygiene, best practices, current cybersecurity vulnerabilities, and trends while training users to better their security capabilities and comprehend the typical actions of cybercriminals. Blockchain technology is used by WBCA to safeguard the software against threats, and it is evaluated and tested using real-world cybersecurity issues with actual users and cybersecurity professionals. The suggested WBCA was also tested on a CentOS-based virtual private server to determine its efficacy, and the authors anticipated that the proposed program might be expanded to other areas, such national or corporate courses, to raise users' cybersecurity awareness levels. At the end, the authors also contrasted WBCA with other cutting-edge web-based cybersecurity awareness program.

In [11], A. Razaque et al. (2021), proposed a blockchain-enabled transaction scanning (BTS) approach for the discovery of anonymous actions that outlines the guidelines for outlier detection and quick currency transfers, which limits aberrant transactional behavior. The BTS method is designed to limit money laundering since using bank cards or money transfers gives terrorist groups and anyone who engage in money laundering new opportunities. The BTS method's prescribed rules determine the distinct patterns of fraudulent activity in transactions, scan the transaction history, and offer a list of entities that receive money in a suspicious manner. The performance of the proposed BTS technique was also verified using a Spring Boot application built by the authors using Java programming. Based on the outcomes of the experiments, the proposed method automates the investigation of transactions and limits the occurrences of money laundering.

In [12], H. H. Alhelou et al. (2021), proposed model using Hilbert-Huang transform and Blockchain-based ledger technology to identify fake data injection attacks (FDIA) in a micro grid (MG) system. By analyzing the voltage and current signals in smart sensors and controllers and extracting the signal features, the model is utilized to improve security in the smart DC-MGs. These networks are susceptible to numerous cyberattacks because of the concurrent growth of DC-micro grids and the employment of sophisticated control, monitoring, and operation technologies, as well as their structure. The authors also considered the outcomes of simulations on various instances in order to confirm the effectiveness of the suggested model. The findings offer that the recommended model can increase the security of data exchange in a smart DC-MG and give a more accurate and reliable detection mechanism against FDIA.

In [13], M. Sadigov et al. (2021), proposed a system-dynamic model of the business's cybersecurity system developed with blockchain technology, giving the capacity to create a computer model of a complicated cybersecurity system for more efficient design. Since 34% of cases are accounted for by system vulnerability due to user behaviors, the authors have placed a strong emphasis on reducing the threat associated with human factors. The goal of the research is to use contemporary BCT to address the problem of rising levels of cybersecurity in big businesses. A causal relationship diagram analysis, differential equations for some of the model's components, and experimental modeling for various values of some parameters at the initial level of others are the foundations of the system-dynamic model, which aims to pinpoint the system sensitivity.

In [14], S. Lee and S. Kim (2021), conducted a survey of official records, interviews, relevant news, technical reports, and research papers from 2016 to 2021, which, by methodically conducting research and analysis, helps to close the gap in blockchain for cyber security. The authors discovered that government-led program and research are both aggressively supporting blockchain, proving that it will play a significant role in cyber protection. Due to its relationship to national security, the cyber defense industry needs advanced security technology. In contrast to conventional systems, blockchain offers strong security features without a

centralized control entity, and its use in the cyber defense industry is receiving attention. With a conclusion of recommendations for future research in elements of the blockchain technology, evaluation, and survey, this work offered prospects that blockchain presents for cyber defense, research, national initiatives, restrictions, and other areas.

III. BCT for Cyber Defense and Cybersecurity

There is a rapid increase in the number of digital populations' worldwide and online businesses every year. Presently, cybercrime has pop up as the enormous security loophole and threat to the global computer information technology industry [15]. The increasing number of online connected devices and online users will ultimately give rise to online crimes, which in turn cost billions of losses to the tech field and companies globally. The digitalization of data and information offers numerous merits but also creates several loopholes and security warnings. The mode of cybercrime is slowly shifting its operating ground from home computers/laptops to mobile phones, tablets, wearable sensors, digital watches, etc. In order to explore the remedies of such threats and provide counter methods to detect or slow down those threats, we have gone through several background studies in the section above.

TABLE I. Summary of Blockchain-based Security and Proposed Models for Cyber Defense and Cybersecurity as Introduced in Background Study and Literature

Ref.	BC model proposed	Author (Year)	Published Paper (Journal/Conference)
[7]	Model for Blockchain-based Agribusiness	N. Kshetri et. al. (2021)	BCT-AA: A survey of Blockchain Technology-Based Applications in context of Agribusiness (SSRN Electronic Journal)
[10]	WBCA (Web-based Blockchain-enabled Cyber Awareness program)	A. Razaque et. al. (2021)	Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain Enabled Cybersecurity Awareness System (Applied Sciences)
[11]	BTS (Blockchain-enabled Transaction Scanning Method)	A. Razaque et. al. (2021)	Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection (Electronics)
[12]	Model to detect FDIA in smart DC-MGs	H. H. Alhelou et. al. (2021)	Cyber-attack detection and Cyber-security enhancement in Smart DC-micro grid based on Blockchain Technology and Hilbert Huang Transform (IEEE Access)
[13]	Blockchain-based System-dynamic model	M. Sadigov et. al. (2021)	Blockchain Technology based System-dynamic Simulation modeling of Enterprise's Cybersecurity System (55th ISC on E&SE)
[14]	Blockchain security for Cyber Defense	S. Lee et. al. (2021)	Blockchain as a Cyber Defense: Opportunities, Applications and Challenges (IEEE Access)

As we have already mentioned, cyber awareness and threat identification play a vital role in combating or fighting against the bad guys or cyber criminals, who are trying to steal/damage online data and secure personal information via various social engineering techniques. We have summarized the blockchain architecture and models (from the Literature Review section of the study) for cyber defense and cyber security in the Table I. The summary includes the proposed model or system with author details and a paper published in the respective conference or journal.

IV. Countermeasures with Blockchain Technology

Based on increasing cybercrimes and cyberattacks reported in Post Covid era, various countermeasures, and security strategies are pointed out as Legal countermeasures, Phase-wise ethics, Minimum use of Autonomous Weapons Systems (AWS), Robot Weaponry (RW) & Autonomous Vehicles (AV), Detecting insider threats from social & online data, Increase cyber capabilities & awareness, and Online gaming prevention and authentication [16] (see Fig. 1). Besides developing legal countermeasures and an increase in military cyber knowledge/power, implementation of phase-wise ethics and minimal use of AWS, RW, and AV will certainly help to counter cybercrimes and cyberattacks. The proposed model by authors (EAMV model as Ethics Authentication Monitoring Verification for online data) is also solely focused on the prevention of cybercrime in post-COVID scenarios. EAMV are described as four firewalls or security processes that hackers have to go through one by one in order to access user data or information.

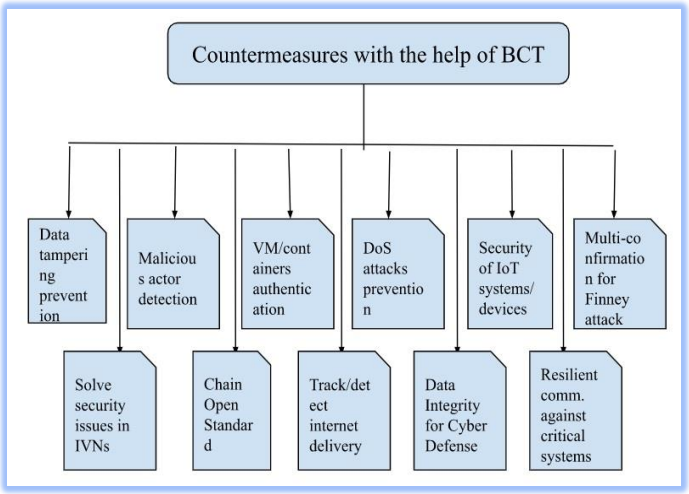

Fig. 1. Various Countermeasures and Cyber Defense Techniques with the Support of Blockchain Technology (BCT) and the Types of Blockchain used for such Countermeasures [16] - [21] [25].

One of the greatest discussed methods for safeguarding data storage, and transfer from decentralized, trustless, peer-to-peer systems is the blockchain. The preliminary keyword explorations by authors highlight blockchain as a standalone technology that carries with it an exorbitant array of possible answers for finance, logistics, healthcare, and cybersecurity [17]. Blockchain uses for cyber security have progressed and bolstered the standing efforts to deter mischievous actors and to boost security. There is an ever-increasing prerequisite to securely cope the cryptography and certification orders as the

WWW transports towards bulk adoption of HTTPS encryption and end handlers are expending it. Ethereum permits for very customizable programming of smart contracts and blockchain uses in the dialectal Solidity. Several major studies alarmed with IoT have offered their own clarifications such as the Proof-of-Possession in the IoTChain proposal.

Not only countering the attacks over the web and malicious actor detection, but a decentralized database of Blockchain on cryptographic practices is also gaining consideration to comfort the security of IoT systems [18]. The blockchain outline within an IoT system is a fascinating auxiliary for old-style database models, which has apprehensions about fulfilling the request for smart home safety. Devices such as door ringlets, light bulbs, control switches, sensor garage doors, etc. are increasing in the marketplace which has limited storage and processing power. Sensors are everywhere surrounded by the home devices via wireless connectivity for remote admission by owners to operate the devices. Design and implementation of a secure home framework model for household IoT devices on Consortium Blockchain (a refined version of blockchain) are experimented with and proposed.

The blockchain perform duties as an immutable log that allows dealings in a decentralized approach. Security threats and existing vulnerabilities to the blockchain systems because of transactions collected into bricks for processing and customary network protocol guarantees each node receives each transaction in close range real-time [19]. Some of the possible and major threats to blockchain systems or blockchain networks are Double-spending security threats, Race attacks, Finney attacks, Brute force attacks, Vector 76 attacks (One confirmation attack), Alternative history attacks, 51% (or > 50%) attack (Majority hash rate attack), Block discarding attack (Selfish mining attack), Block-withholding (BWH) attack, and Fork-after-withholding (FAW) attack. Possible countermeasures for the mentioned attacks include (i) installing observers in the web, communicating binary spending cautions among groups; (ii) waiting for multi-confirm actions for transactions; (iii) informing the merchant about an ongoing binary consume in the network; (iv) disincentive huge mining reserves, twinsCoin, PieceWork; (v) ZeroBlock technique, a timestamp-form technique such as bloomness preferred, DECOR+ protocol; (vi) involve only familiar and committed miners in the pool, cease and terminate a pool when revenue sinks from calculated or sudden change occurs; and (vii) use of cryptographic commitment schemes.

The connection amid the vehicular network and the exterior world has several security pigpens that hackers can be custom to abuse a vehicular network. Some popular protocols for in-vehicle networks (IVN) are Controller Area Network (CAN), FlexRay, and automotive Ethernet, which are not designed with security in concentration. A blockchain is a noble approach to solving standing security issues in IVNs and using hybrid blockchain, there exist several ways to improve IVN security [20]. Protocols used for IVNs have numerous vulnerabilities, such as a shortage of message authentication, a shortage of message encryption, and an ID-based arbitration appliance for conflict determination. Sophisticated attacks by hackers can be launched that may clue to the loss of property and lives using these vulnerabilities. Although several algorithms were proposed in the past for IVN intrusion detection, there are several limitations to the proposed algorithms.

Blockchain technology has cracked two major problems of the digital economy - (i) once assets are digitized, movement can be over the chain, and (ii) zero-trust cost under anonymous societies for innovative chances for the internet economy. BCT is a double-edged weapon for old-fashioned economic and financial progress that places a high demand on data handling and risk-response capabilities [21]. The ultimate goal of BC is to analyze and process information through the active integration of financial funds. BCT can benefit the financial industry to automatically and accurately detect customer credit conditions to restructure the financial shop credit system and progress the efficiency of cross-border payment. To advance the blockchain financial and economic provision quality, smart contracts can be measured in order to track criminal activities. Supervision of financial firms appealing in financial derivatives ought to be strengthened; management authorities must stipulate the bottom capital of financial firms.

V. Advantages of Blockchain Technology W.R.T. Cyber-Defence and Cyber-Security

Blockchain technology is one of the popularly noted and known terms nowadays in the field of secure transmission of credential data over the internet. Each block contains user data with high secure hash code as well as the previous block hash code and forms a secured chain. Any unauthorized accessibility can be easily detected in blockchain technology. With its strong security policy, this technology uses in many areas like Markets (Billing, Marketing, etc.), Government Sector (Document digitization / Contracts, Voting, Registries etc.), IOT (Self-driving cars, personalized robots) [27] , HealthCare systems, Finance, and Accounting and many more.

As we know that in the current scenario where the number of internet users increased day by day, the number of cyber-attacks also increased comparatively [28]. The actual data of a user is threatened by the attacker and used in an unauthorized manner. So, blockchain technology with its security mechanism helps to increase the security in cyber-attacks. The use of this technology has many advantages over cyber defense [29] and cyber security [30] which are categorized in the Table II and Table III.

TABLE II. ADVANTAGES OF BLOCKCHAIN TECHNOLOGY W.R.T. CYBER DEFENSE THAT HELPS TO INCREASE SECURITY IN CYBER-ATTACKS [27] - [31]

S.N.	Security aspects of BC	Advantages over Cyber Defense
1	Decentralized data	It reduces possible attacks. The attackers did not know where the actual data was stored.
2	Traceability	It increases the cyber defense approach by easily tracing which block gets infected and prevents it.
3	Strong Encryption	A strong encryption mechanism using hash code increases cyber defense.
4	Transparency	Transactional data can be digitally authorized and accessible by all the members of the network.
5	No Setup and maintenance of h/w, s/w	No additional security infrastructure is placed for cyber-attacks.

TABLE III. ADVANTAGES OF BLOCKCHAIN TECHNOLOGY W.R.T. CYBER SECURITY THAT HELPS TO INCREASE SECURITY IN CYBER-ATTACKS [27] - [31]

S.N.	Security aspects of BC	Advantages over Cyber Security
1	Secured Data	User credential data is secured in blocks with high-security hash codes. It reduces cyber-attacks and increases security.
2	Unchangeable transactions	The insertion of new blocks in a chain cannot be removed or modified. Not an easy task for attackers to change the block data or address.
3	Prevention of Fraud	The consensus approach prevents it from external access and cyber-attacks.
4	No middleware security breach	Data transfer from sender to receiver without the need of mediating third parties. So, in the middle attacks get reduced.
5	No Single point failure	Any type of network or cyber-attacks will not generate any type of data loss because of multiple copies of data at different sites.

VI. BLOCKCHAIN-BASED SOLUTIONS AND CHALLENGES

Keeping transparency and trust as vital drivers, blockchain technology might be a hopeful technology. Findings illustrates that BCT has the ability to aid transparency and build citizens' trust in community deal delivery while continuing a sufficient level of privacy [32]. Transparency of evidence and procedures shows a vivacious role in gaining the citizens' trust. Blockchain has a disrupting role in handling transparency, trust, citizen satisfaction, and reducing corruption in order to develop the efficiency of civic service delivery.

Although there are several solutions proposed and used by Blockchain for Cybersecurity and Cyber Defense, there are also huge challenges while embedding blockchain solutions on the other end. To come up with exact blockchain solutions and ongoing challenges and issues, we have summarized the blockchain challenges and blockchain solutions in the Table IV with respect to cybersecurity, cyber defense, and countermeasures.

TABLE IV. BLOCKCHAIN-BASED SOLUTIONS AND BLOCKCHAIN-BASED CHALLENGES FOR CYBER DEFENSE AND CYBERSECURITY WHILE INCORPORATING THE SOLUTIONS [17] - [26]

SN	Ref. (Year)	Solution domain(s)	BC Type	BC solutions for cybersecurity & cyber defense	BC challenges while incorporating those solutions
1.	[17] (2019)	Sidechain Security, IoT Security	Public & Private	Deployed to decipher problems related to the safety of devices, networks, and users. Cryptocurrency is preserved through a Proof-of-Work (PoW) tool.	A decentralized, trustless system cannot by this one crack all glitches in cybersecurity. Need to strongly succeed the adjoining cryptography and certification patterns.
2.	[18] (2020)	Smart Home Security	Consortium	Blockchain framework (for a secure smart home within an IoT system), a decentralized database, as a substitute to traditional centralized database models.	The complexity to instrument smart contract results possibly can rise the system fee. Public blockchain design is not suitable for smart homes owing to scalability.
3.	[19] (2018)	Privacy and Transaction Security	Public, Private & Consortium	Contains a certifiable record of each and every transaction ever finished in the system. BC is a distributed sleeve system where contestants keep replicas of files and approve on the alterations by consensus.	Despite the giant opportunities BC compromises, it undergoes from challenges and limitations such as scalability, privacy, compliance, and government disputes that have not been discovered and addressed.
4.	[20] (2021)	In-Vehicle Network (IVN) Security	Hybrid	BC is a good approach to solving existing security issues in in-vehicle networks (IVNs). A suggested way to develop IVN security is constructed on a hybrid blockchain.	Hybrid BC framework for securing in-vehicle webs uses private BC to shelter message flows between sensors and components inside the vehicle and open BC for connecting which is insecure.
5.	[21] (2018)	Finance & Economics (Cross-Border Payment Security)	Public & Private	The goal of BC in the internet era is to analyze and route data through the current integration of financial services. BC can exactly identify consumer credit situations to rearrange the market credit system &advance cross-border payment efficiency.	The weak foundation of related research, difficulties encountered, and finance applications of BC are in their infancy in countries. Governments and countries should build a general-purpose application facility platform for enterprises via BC.
6.	[22] (2020)	Electronic Health Record (EHR) Security	Private	The properties for protected EHR systems (like Data accuracy & integrity, Data privacy, Efficient data sharing, Control return of EHRs back to	Has numerous restrictions and aggressive extensions will need fundamental protocol redesign. Personal healthcare figures collected are tall in volume and at

				patients) can be accomplished using blockchain as Decentralization, Security, Pseudonymity, Immutability, and Autonomy.	reckless rate. It could lead to high network invisibility due to physical space& traffic congestion. Also, mining process may cost great, limit blockchain use.
7.	[23] (2018)	Cloud-Based Data Security	Public & Private	BC is secure by policy that provides the aptitude to achieve decentralized consensus and consistency, and resilience to planned / unplanned attacks with crucial benefits (settlement without mediator, patient's control).	Strong data integrity outcomes in immutability (data cannot be reformed or deleted). One of the ethics of privacy standard, based on data safety laws, provides the right-to-erasure to folks. Healthcare data can be huge and requires examining.
8.	[24] (2017)	Automotive Security and Privacy	Private	BC based architecture to shelter the user's privacy and to upturn vehicular ecosystem security with evolving services like dynamic vehicle insurance charges and wireless remote software modernizes.	Some of forthcoming research challenges include the Key management (each vehicle owns several communication key with users which may alter) and Data caching (vehicle must take data from cloud, that suffers overhead and interval).
9.	[25] (2016)	National Defense (Cyber-enabled defense systems)	Private	BC work independent of security and trust by conserving truths in dual ways – (i) ensure digital dealings on BC network, (ii) via consensus, events are safe in database, without modification.	Narrow awareness/knowledge of blockchain technology and need to create a line of research to confirm scalable, adaptable, and securable to back missions in air, space, and cyber domains.
10.	[26] (2018)	Electric Vehicles, Cloud and Edge Computing Security	Public & Private	Built on distributed consensus, BC-inspired data coins and energy coins are suggested where data contribution occurrence and energy contribution volume are applied to triumph the proof of work with security results for vehicular exchanges.	Proof grit via data contribution occurrence and energy contribution amounts can stance challenge and reply due to secret data transmission via sensors. EV and sensors will be charged by wired and wireless skill and trading coins can be risky.

VII. Conclusion and Future Scope

We have presented a comprehensive survey of how blockchain technology can be useful to provide security over the web/internet and can be used to counter ongoing cyber threats as well as increasing cybercrimes and cyber-attacks. We have summarized the recent blockchain models and architectures used for cyber defense and cybersecurity. Various countermeasures and cyber defense techniques from "prevention of data tampering" to "detecting internet delivery" have been analyzed and discussed. We conclude that blockchain technology can have several advantages over cybersecurity and cyber defense with various security aspects like traceability, encryption, transparency, data security, unchangeable transactions, fraud prevention, no single point failure, and no setup/maintenance of hardware/software etc. We also pointed out several challenges and solutions (blockchain-based), with particular blockchain types like public, private, hybrid, and consortium Blockchain that can act as recommendations for improvement on integrating blockchain with cyber defense and cybersecurity.

There is no doubt that Blockchain technology has already been used in many fields, especially finance, supply chain, digital advertising, IoT Security, and many more. Due to its unique properties, the scope of blockchain technology in the zone of cybersecurity and cyber defense can be revolutionary. Despite its open and public nature, data can be verified and encrypted using the most secure cryptographic technology which makes the authorization access of data or information impossible. The key strength of blockchain technology is decentralization property that highly increases the capabilities of the system in making security decisions of its own. The technology is most likely to be used in IoT and Networking Security, Secure Data Transmission, Securing DNS, Securing Data Storage, Verification of Cyber-Physical Infrastructure, and many more.

Acknowledgment

We would like to thank all the brains who helped directly & indirectly in writing/completing this paper.

References

[1] https://www.ironnet.com/topics/what-is-cyber defense#:~:text=Cyber%20defense%20is%20a%20coordinated,that%20occur%20within%20a%20network. Accessed on 25/09/2022.

[2] S. Lee, & S. Kim, "Blockchain as a Cyber Defense: Opportunities, Applications and Challenges", IEEE Access, 10, 2602-2618,2021.

[3] D. Galinec, D. Možnik, & B. Guberina, "Cybersecurity and cyber defense: national level strategic approach", Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije, 58(3), 273-286, 2017.

[4] C. Solar, "Cybersecurity and cyber defense in the emerging democracies", Journal of Cyber Policy, 5(3), 392-412, 2020.

[5] Y. Li, & Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", Energy Reports, 7, 8176-8186, 2021.

[6] C. S. Bhusal, "Blockchain Technology in Agriculture: a case study of blockchain Start-up Companies", Int. J. Comput. Sci. Iinf. Technol., 13(5), 2021.

[7] N. Kshetri, C.S. Bhusal, & D. Chapagain, "BCT-AA: A survey of Blockchain Technology-based Applications in context with Agribusiness.", DOI: https://dx.doi.org/10.2139/ssrn.3834004, Available at SSRN 3834004, 2021.

[8] E. Piscini, D. Dalton, & L. Kehoe, "Blockchain & Cyber Security", https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf, accessed on 02/10/2022.

[9] O. Lage, S. de Diego, B. Urkizu, E. Gómez, & I. Gutiérrez, "Blockchain applications in cybersecurity. Computer Security Threats", 73, 2019.

[10] Razaque et. al. "Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain Enabled Cybersecurity Awareness System", Applied Sciences 2021, 11, 7880. Published: 26 August 2021, DOI: https://doi.org/10.3390/app11177880.

[11] Razaque et. al. "Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection", Electronics 2021, 10, 1766. Published: 24 July 2021, DOI: https://doi.org/10.3390/electronics10151766.

[12] Alhelou et. al. "Cyber-attack detection and Cyber-security enhancement in Smart DC-micro grid based on Blockchain Technology and Hilbert Huang Transform", IEEE Access 2021, Vol- 9. Published: 12 February 2021, DOI: https://doi.org/10.1109/ACCESS.2021.3059042.

[13] Sadigov et. al. "Blockchain Technology based System-Dynamic Simulation Modeling of Enterprise's Cybersecurity System", 55th International Conference on Economic and Social Development - Baku, 18 - 19 June 2020, Vol. 1/4, P. 399-408. URI: https://essuir.sumdu.edu.ua/handle/123456789/85701.

[14] Lee et. al. "Blockchain as a Cyber Defense: Opportunities, Applications and Challenges", IEEE Access 2022, Volume 10. Published: 16 December 2021, DOI: https://doi.org/10.1109/ACCESS.2021.3136328.

[15] Almiani et. al. "Deep current neural network for IoT intrusion detection system. Science Direct, Simulation Modeling Practice and Theory", Volume 101, May 2020, 102031, DOI: https://doi.org/10.1016/j.simpat.2019.102031.

[16] N. Kshetri and A. Sharma, "A review and analysis of online crime in pre & post COVID scenario with respective counter measures and security strategies", Journal of Engineering, Computing & Architecture (JECA),ISSN: 1934-7197, Volume: XI, Issue: XII, December 2021, DOI: https://doi.org/17.0002.JECA.2021.V11I12.200786.7902.

[17] KKR Choo et. al (2019). "A systematic literature review of blockchain cyber security, Digital Communications and Networks", ScienceDirect, Volume: 6, Issue: 2, May 2020, Pages: 147-156, DOI: https://doi.org/10.1016/j.dcan.2019.01.005.

[18] M. Imran et. al., "Investigating smart home security: Is Blockchain the Answer? IEEE Access, Special Section on Blockchain-Enabled Trustworthy Systems", Volume: 8, Pages: 117802-117816, 2020, DOI: https://doi.org/10.1109/ACCESS.2020.3004662.

[19] N. Rathod and D. Motwani, "Security threats on Blockchain and its countermeasures", International Research Journal of Engineering and Technology (IRJET) Volume: 05, Issue: 11, e-ISSN: 2395-0056, November 2018, Pages: 1636-1642, DOI: IRJET-Security-threats-on-BC-and-its-countermeasures.

[20] SY Nam et. al., "Security issues with In-Vehicle Networks, and Enhanced Countermeasures based on Blockchain", MDPI Electronics 2021, Volume: 10 (Issue: 8), Pages: 893. Published: 8 April 2021, DOI: https://doi.org/10.3390/electronics10080893.

[21] Y. Zheng and T. Huang, "The Challenges and Countermeasures of Blockchain in Finance and Economics", Systems Research & Behavioral Science (SRBS), Wiley Online Library, Volume: 37, Issue: 4, Special Issue: Industry 4.0, July/August 2020, Pages: 691-698, DOI: https://doi.org/10.1002/sres.2710.

[22] D. He et. al., "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security", Elsevier Ltd., 2020, DOI: https://doi.org/10.1016/j.cose.2020.101966.

[23] C. Esposito et. al., "Blockchain: A panacea for Healthcare cloud-based data security and privacy?", IEEE Cloud Computing, Jan/Feb 2018, Department: Cloud and the Law.

[24] A. Dorri et. al., "BlockChain: A distributed solution to Automotive security and privacy", IEEE Communications Magazine, December 2017, DOI: 10.1109/MCOM.2017.1700879.

[25] N. B. Barnas, "Blockchains in National Defense: Trustworthy systems in a Trustless World", Air University, Maxwell Air Force Base, Alabama, June 2016.

[26] H. Liu et. al., "Blockchain-enabled security in Electric vehicles cloud and Edge computing", IEEE Network May/June 2018, DOI: 10.1109/MNET.2018.1700344.

[27] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, Ben Amaba, "Blockchain technology innovations. IEEE Technology & Engineering Management", Conference (TEMSCON).

[28] Kshetri, N., "The global rise of online devices, cybercrime, and cyber defense: Enhancing ethical actions, counter measures, cyber strategy, and approaches", University of Missouri – Saint Louis, ProQuest Dissertations Publishing, 29165177, May 2022, DOI: https://dx.doi.org/10.13140/RG.2.2.33257.57446,

[29] Suhyeon Lee, Seungjoo Kim, "Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges", IEEE Access, Volume: 10, 2021.

[30] A. R. Mathew, "Cyber Security through Blockchain Technology", International Journal of Engineering and Advanced Technology (IJEAT), 2019.

[31] K. Anderson, Capterra, "The benefits of Blockchain for IT, Part 2: Cybersecurity", Published: 6 Jun 2018, https://blog.capterra.com/benefits-of-blockchain-cybersecurity.

[32] Kshetri, N., "Blockchain Technology for Improving Transparency and Citizen's Trust", In: Arai, K. (eds)Advances in Information and Communication (book series AISC, Volume - 1363), FICC 2021, Springer Nature Switzerland AG 2021, Page: 716-735, DOI: https://doi.org/10.1007/978-3-030-73100-7_52.

AUTHORS' PROFILE

Dr. Naresh Kshetri (Member, IEEE) is currently an Assistant Professor of Cyber Security at Lindenwood University, USA. He completed his Master of Computer Applications (MCA) from University of Allahabad, MS (Cybersecurity) from Webster University, and PhD (CS) from the University of Missouri–St. Louis (UMSL), Missouri, USA. He also worked as a graduate teaching assistant/graduate research assistant for the computer science department, UMSL besides working as an Adjunct Instructor (CS) at Lindenwood University. With nine+ years of experience in teaching and research, he has a total of eight publications *(all as first author)* in reputed journals, conferences/book chapters. His current research interests include blockchain technology and cybersecurity. For more about Dr. Kshetri, please visit: https://sites.google.com/view/nareshkshetri.

Chandra Sekhar Bhushal is a Master graduate from Federation University, Australia majoring in Software Engineering in the year 2020. He has also completed a Master of Computer Application (MCA) from Visvesvaraya Technological University (VTU), India (2015). He has 1.5 years of experience in teaching. He has a total of three publications in the International Journal. His current research interests include information security, social engineering, cybersecurity and blockchain technology.

Dr. Purnendu Shekhar Pandey has done his Ph.D. from IIIT-A (Indian Institut e of Information Technology, Allahabad) in Information Technology. He worked in various Government and private institutions. Presently he is working as an Associate Professor in the Department of Computer Science & Engineering, KIET, Group of Institutions, Ghaziabad, U.P. His areas of research are mainly in the field of IoT, Machine Learning, Cyber-Security, Sensor Networks, Network Coding, D2D assisted Networks, etc. He has published various papers in SCI and ESCI Journals, top-notch conferences like ANTS, FRUCT, NOPE, and CCNC (h-index> 25), and reviewer in various peer-reviewed SCI journals. He has given various talks on IoT and discrete process modeling, machine learning in industrial IoT, etc. in various national and international conferences and has hosted various session chairs at various international conferences.

Vasudha is currently working as an Assistant Professor in the Computer Science Department at United Institute of Management Naini, Prayagraj, Uttar Pradesh (India). She has done MTech (Computer Science and Engineering) from Dr. A.P.J. Abdul Kalam Technical University Lucknow, Uttar Pradesh in the year 2018. S he has also completed Masters in Computer Science (MCA) and Bachelor in Computer Science (BCA) from Integral University, Lucknow (U.P.) in the year 2014 and 2011 respectively. She has published two Conference Proceedings papers conducted by IEEE. Her research area is image processing, database security, cybersecurity and blockchain technology.