Blockchain in Indian National Defence

Dinesh K. Choudhary[1] Shanthi Bhatt[2]
[1]MCA Student [2]Professor
[1,2]Department of Master of Computer Application
[1,2]SIESCOMS, India

Abstract— The ability of the Indian Armed Forces to prevail in the highly contested environment of 2040 will be dictated by its ability to defend cyber-enabled systems, and the data within them, from compromise and manipulation. Yet contemporary cyber defense is faltering, and incremental improvements seem unlikely to overcome an exponentially growing cyber threat. Thus, an entirely new model for cyber defense strategy is needed. Blockchains are a new information technology that inverts the cyber security paradigm. First, blockchain networks are trustless; they assume compromise of the network by both insiders and outsiders. Second, blockchains are transparently secure; they do not rely on failure-prone secrets, but rather on a cryptographic data structure that makes tampering both exceptionally difficult and immediately obvious. Finally, blockchains networks are fault tolerant; they align the efforts of honest nodes to reject those that are dishonest. As a result, blockchain networks not only reduce the probability of compromise, but also impose significantly greater costs on an adversary to achieve it. The Indian Armed Forces should research and develop blockchain technology and leverage it for national defense.

Key words: Military Equipement, Aerospace Safety, Blockchain, Main-Net, Indian National Defence, DoD, Security, India, DRDO, Block, Private Network

I. INTRODUCTION

Blockchain technology is a distributed transaction technology that is open but secure and public but at same time private.

It works on three main principles:

1) The transaction is opened on the network.
2) The ledger is distributed to ensure there is always a copy of the ledger.
3) Every new transaction needs to be authenticated to be added to the chain.

It was built from the three technologies -

1) Private Key Cryptography,
2) P2P network and
3) Program (the blockchain protocol).

The private key cryptography provides a powerful ownership tool that fulfills authentication requirements. Possession of a private key is ownership. It also spares a person from having to share more personal information than they would need to for an exchange, leaving them exposed to hackers. Authentication is not enough so, Authorization - having enough money, broadcasting the correct transaction type, etc - needs a distributed, peer-to-peer network as a starting point. A distributed network reduces the risk of centralized corruption or failure.

II. HISTORY OF ARMED FORCES SECURE NETWORK

The story of cyber defense is a tragic tale that begins in 1988 with the ARPANET, the precursor to the modern internet. It is tragic because many of the flawed assumptions and philosophical leaps that underpinned cyber defense then still apply today. Understanding the architecture and governance structure from ARPANET can help to illuminate shortfalls in modern cyber defense, and provide a guiding policy for creating a new defense strategy based on modern technology. In 1962, engineers from the Defense Department's Advanced Research Projects Agency (ARPA) began work on the precursor to the modern internet: the ARPANET.[16]

The only rules that governed the network were embedded in the communication protocols that allowed the various nodes to communicate. Governance of the network, however, was centralized through DARPA and a number of formal working groups that oversaw ARPANET's technical development and implementation. In other words, ARPANET used the principle of centralized control and decentralized execution.

III. CURRENT DOD DATA SECURITY IN INDIA

Cyberspace is now as relevant a strategic domain as are the other four naturally occurring domains of land, air, sea and space. As the Union Minister for Defence Manohar Parikkar recently highlighted, India's defence capabilities must be[1].

In 2015, 72 percent of Indian firms faced at least one cyber-attack.[2] Critical information infrastructure in India has also been subject to espionage campaigns like the Ghost net hacking of Defence Research and Development Organization computers in 2012.[3] By one estimate, India was among the countries most targeted by cyber criminals through social media in 2014.[4] According to data from the Computer Emergency Response Team (CERT), some 8,311 security breach incidents were reported in the country in 8 January 2015, as against 5,987 in November 2014.[5] Meanwhile, the number of websites 'defaced' during the same period increased from 1,256 to 2,224. The CERT report ranked India as the third most vulnerable country in Asia for 'ransomware' attacks (malware that curtails access to the infected device in return for a ransom).

The cyber threat is not just growing; it is growing in three distinct ways. In the future, the Indian Armed Forces will face an array of cyber forces that are more numerous, more capable, and better resourced than those it faces today. The number of devices projected to become part of the "internet of things" (IoT) is staggering. In 2006, there were two billion internet-enabled devices in use, or 0.3 devices for every person on Earth. By 2020, Cisco and Intel project that number could grow to 50-200 billion devices, respectively, or 6.5-26 devices per person.[15]

TOP SECRET and SECRET Information in Electronic Form.

A. Top Secret Information in Electronic Form.

1) Classified information of SECRET and above will not be stored permanently on a computer. An exclusive standalone computer along with exclusive printer under the ownership of an officer will be used for creating such document and will be securely erased after printing required number of copies. It will be ensured that there is no data remaining in the originating computer including page files, swap areas, slack areas, RAM etc.
2) A register will be maintained for this exclusive printer to record number of copies printed.
3) Under NO circumstances, SECRET and above data will be typed or viewed on Computers of PA/Steno or computers connected on WAN/LAN/ Army One Network etc
4) Secure erasing software's like ERASER (latest version) or Secure Desk V2.0 may be used to securely delete such classified data files from the originating computer. Instructions for Backup of SECRET Digital Documents. It is advisable to keep only hard copies of SECRET and above documents. However, in case it is inescapable, it should be stored on CD/DVD or any other authorized external storage media and kept under lock and key.

B. The procedure for ensuring the data integrity of the classified information is as under: -

1) A hash signature of the secret digital document along with the document will be encrypted and then burnt to the CD/DVD.
2) The password for encryption will be sealed in an envelope and will be handled in accordance with the security classification of the document concerned.
3) Record of all such CDs along with hash signatures (numbered and stamped) will be maintained in a register by the originating officer.

C. Information up to Confidential in Electronic Form.

1) All documents/presentations will only be created and processed on standalone computer of the branch/department. Confidential data will not be created on computers connected to WAN/LAN/ Army One Network etc
2) Network/Transport Layer Security. The applications developed will include mechanisms to secure classified information through network/transport Layer, Virtual Private Network (VPN), implementations such as Secure Socket Layer (SSL)/Transport Layer Security (TLS) between the information processing nodes / endpoints.
3) Application Layer Security. Application level encryption will be ensured during development of applications between end users (i.e. desktop to desktop application security). Application level security between end users will be applicable to all types of media i.e. both radiating as well as non-radiating. Application layer security design for customised software applications must include commercially available Public Key Infrastructure (PKI) solutions in the initial framework itself.

IV. ATTACKS ON DEFENCE NETWORKS

There are many attacks are done by various hackers on the Defence organizations, they are Government as well as private. Some are defence giant like Lockheed Martin and Boeing also Government organization like US Ministry of Defence in Pentagon. Indian organization like "Defence Research and Development Organization (DRDO)" also hacked. Many times government websites are also hacked by different local hacker groups from Pakistan and China.
Some are following notable hacks:-

1) In January 2015, Edward Snowden revealed China stole designs for the US-built F-35 Fighter jet hacking computer systems at US Defense contractors, and provides details also a counter-intelligence operation run by the NSA. The hackers aimed to steal blueprints and intellectual property for the F-22 and F-35 fighter jets and C-17 transport aircraft. The purpose of the Chinese Government is to acquire intellectual property on advanced technologies, benefiting Chinese companies on the market and narrowed the gap in the research of advanced technological solution. Military experts speculated that the stolen blueprints could help the country to develop a new generation of advanced aircraft fighter, so-called "fifth-generation" fighters. Chinese hackers exhilarated 65 gigabytes of data over a couple of years.[9]
2) In December 2013 in DRDO around 50 computers belonging to the armed forces and the DRDO were hacked sometime back and classified files could have been compromised. Source said that around up to 30 files marked as classified could have been compromised in the process of the hacking. An advisory issued to the Services said that it was found that a spyware was detected which could read the files of computers, which were not even connected to internet.[10]

V. WHY BLOCKCHAIN MATTERS

Blockchains solve a challenging problem in data science of reliably exchanging information over an unreliable network on which some of the participants cannot be trusted.[18] The blockchain security model inherently assumes that these dishonest participants will attempt to create friction by not only generating false data, but also by attempting to manipulate valid data passed from honest participants.[19] By using a variety of messaging and consensus techniques, blockchains ensures data integrity by both rejecting invalid data and preventing valid data from being secretly modified or deleted. blockchains ensures data integrity by both rejecting invalid data and preventing valid data from being secretly modified or deleted.

blockchains are capable of operating successfully and securely on the open internet, without a trusted central authority, and while fully exposed to hostile actors. Given their ability to protect the integrity of data in spite of adversary actions, blockchains offer significant military utility to the Indian Armed Forces to prevail in the highly contested environment of 2040.

Like most technology Blockchain is also combination of most recent and powerful technology combine one powerful and unique technology which has more functions and compatibility. The some of various technology are follows.

A. Hashing

Hashing means taking an input string of any length and giving out an output of a fixed length. In the context of cryptocurrencies like Bitcoin, the transactions are taken as an input and run through a hashing algorithm (Bitcoin uses SHA-256) which gives an output of a fixed length.[20]

Let's see how the hashing process works. We are going put in co-ordinates of Mumbai city (18°58′30″N 72°49′33″E)[21]. For this exercise, we are going to use the SHA-256 (Secure Hashing Algorithm 256).

Input Coordinates	Output Hash
18°58′30″N 72°49′33″E	41E1A594D9364C11DFD156D5B34F31FA34CC11D4D5D2685C11191795991BC1B

Table 1: Mumbai coordinates are hashed with SHA-256 done by [22]

B. Block Structure and Its Contents

A blockchain is a database composed of "blocks" (e.g., a group) of records, with each block containing a cryptographic link to the previous block, forming a chain. A blockchain begins as a single block, sometimes called the genesis block.

[23] As new blocks are added they are "stacked" on top of the previous block. A visualization of a blockchain can be seen in Figure 2. Blockchains can be compared to pages in a book.[24] Each block, or page, has a header (e.g, identifying information at the top of the page) and contents (e.g., text). The header of each block contains several pieces of information, but only three are highlighted here. First, and most importantly, is the digital fingerprint, or hash, of the previous block. Next is a timestamp that denotes when the block was created. Finally, there is the hash of the block's contents.[25]

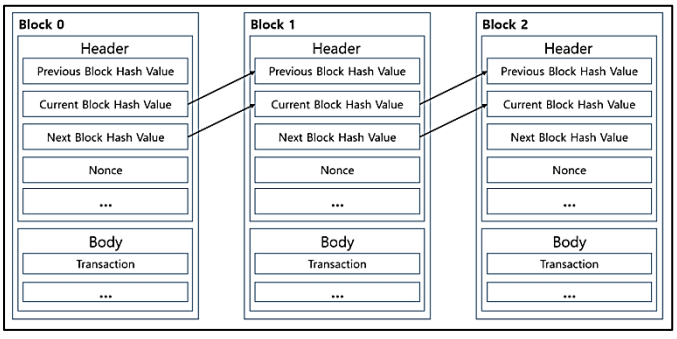

Fig. 1: Block structure

1) Network Architecture

Blockchains can be established on a variety of network architectures ranging from completely centralized to completely distributed, as illustrated in Figure 3.It is important to note, however, that each of these network architectures represent trade-offs in security and efficiency. For instance, in a centralized network,. At the other end of the spectrum is the distributed network, where each node is functionally independent from any other node. As a result, the compromise of individual distributed nodes does not necessarily compromise of network as a whole.[27]

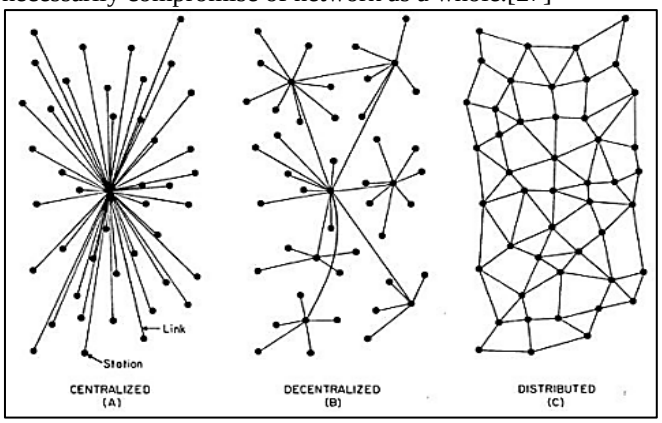

Fig. 2: Diagram of generic network topologies [26]

C. Network Nodes Types

Network nodes serve as both the users and defenders of the blockchain. As users, they bothgenerate new records to be included in the blockchain and reference the blockchain for historical information. Network nodes defend the blockchain by participating in the consensus mechanism, although not all nodes need participate in every aspect of consensus, depending on access control, for instance. The types of nodes in any blockchain network will vary depending on the network's purpose. In an Air Force context, nodes could be envisioned in three categories, depending on their relative capability (e.g., processing, storage, communication, etc).

Type	Example	Responsibilities (rank ordered)
Full	Server/Desktop Tactical platforms GEO Satellites Indian Naval Ships control Room AWACS Strategic Helicopter	Independent constructs complete copy of blockchain Generating Blocks Verifies Blocks Verifies all records Generate and transmit new records
Partial	Laptop LEO Satellites Small UAV Small Tactical Naval Ships Small Tactical Helicopters	Construct "headers-only" copy Verifies new block Verify new records Verify old records with peer support Generate and transmit new records
Simple	Cellphone Attritable UAV Tactical Personal Systems	Verify new records Generates and transmits new records

Table 2: Example of blockchain node types in an Defence network

These categories include Full Nodes, Partial Nodes, and Simple Nodes. Examples and responsibilities of each node type are summarized in Table 3. Full Nodes serve as the backbone of the blockchain network. Their most important function is to build and maintain a complete, up-to-date copy of the blockchain database. Another important function performed by full nodes is generating new blocks, which are then distributed to other nodes. Next, full nodes

will verify new transactions or blocks received from other nodes, ensuring they are in accordance with the consensus rules and maintain the database's internal consistency. Finally, like all other nodes, Full Nodes generate and transmit new records for inclusion in the database.

VI. How Blockchai can be useful in National Defence

Blockchain technology is a distributed transaction technology that is open but secure and public but - at same time -private. It is initially created to provide a distributed ledger of financial transactions whereas every new transaction needs to be authenticated to be added to the chain. One of the most important things is that blockchain technology is important to Department of Defence (DoD). To save their data such as Legal contracts, Defence Personals data, Important Mission data, experimental weapon system technology, communication data. Blockchain implementation in DoD data will lead to more interoperability of data access and security of data. Blockchain technology has an ability to make dramatically changes in security of country. This paper describes about the current issues of data security of DoD in India and how blockchain technology can useful for Government to improve the data security and improved access to the soldier and defence personal in India.

For national defence there need to be some blockchain which are not publicly to everyone but for some which are authorized to use it and store data on it. Some images below show the structure of the proposed Blockchain Framework architecture for Department of Defence.

A. Login to the Private Network

In below Image shows how client can login to private network. Client needs to login with credentials on the interface on the system and then proof the user is valid, no other person is using valid persons credentials to login in private network. For this we can use Iris scanner, Fingerprint scanner or better way is RSASecureID with fingerprint scanner which helps to prevent the private network from unauthorized access.

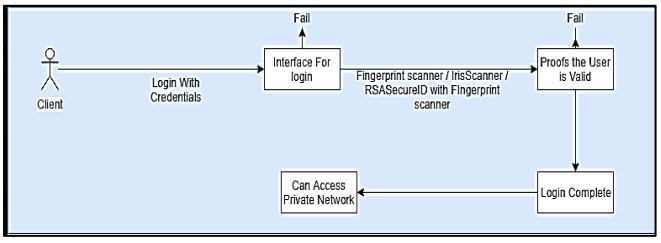

Fig. 3: Login to the private Network

B. Login to Main-Net to access data on Blockchain

In the below image shows once client /User enter into private network then only he can access the blockchain netwok(Main-Net). To access the Main-Net he needs to register his system to the Main-Net for that client requires credentials and required certificates and private key to register. There is small group of nodes(peers) are responsible for validating client and its certificates and define its access level and permission level. That small net is a combination of system which are not using the Main-Net and not performing any transaction on the Main-Net.

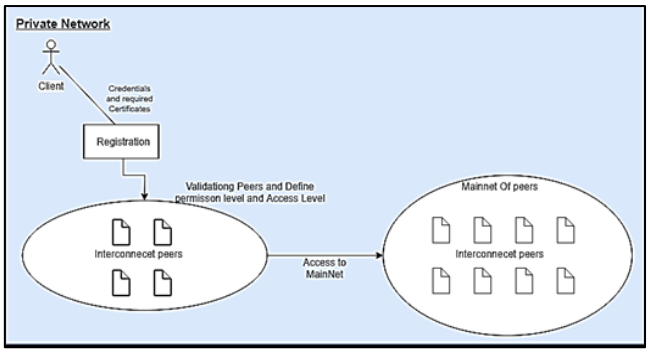

Fig. 4: Login to the Main-Net to access Data

C. Creating a block on Main-Net

In the below Image shows how blocks will be created and verified by other nodes/Peers on the network. The block contains a data to add to blockchain. Once verifies the data by the nodes the block is attached to the Blockchain.

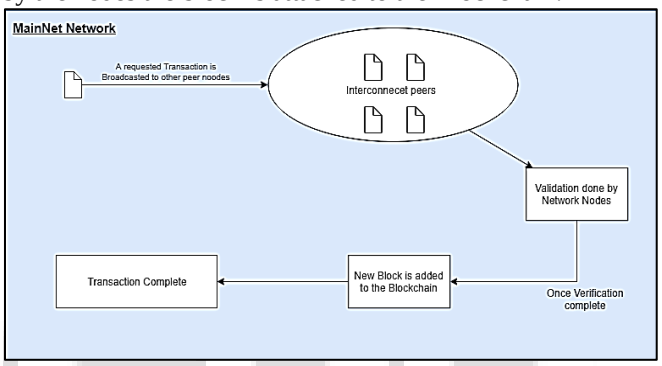

Fig. 5: Creating a block on Main-Net

D. Reading Block of Data on Blockchain

A request to read data from blockchain is made to the other nodes. Validation done by the Network nodes with complex algorithms and access level of nodes. Once the request is verified data(block) provided to the client.

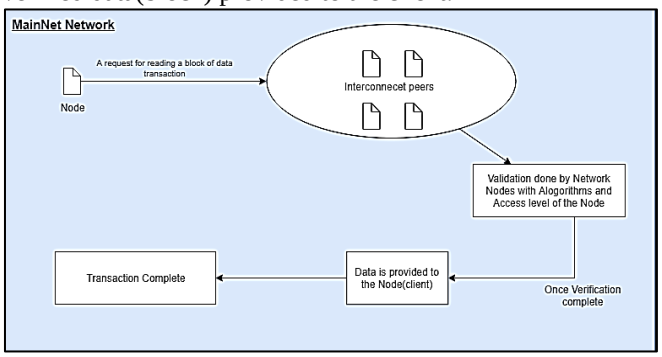

Fig. 6: Reading a block of data on Blockchain

A block can be thought of as a bundle of transactions, with each transaction needing to be validated before it can be accepted by the network. Each block has what is known as a block size. The block size is simply the maximum limit a block can be filled up with transactions. For example, the Bitcoin block size currently stands at 1 MB. Miners can choose how much of a block to fill with transactions.[30] However, if a block that exceeds the block size limit is submitted, then the block of divided into multiple block and these blocks are linked to previous and next block, so that all blocks are connected and in a serial manner. Dynamic block size limit. What this means is, the block size limit changes by itself and is dependent on the

data(transaction) volume at any given time. A blockchain-based network that uses a dynamic block size limit enjoys the benefit of being less prone to a slowdown in its network. If block of data is small to the block in which it is going to store data then dynamically that block size reduces. The defence network is strong and with good bandwidth of Internet hence in this Main-Net the block size should be varying from 1MB to 50MB depends on the node(peer) on which block is running. The below table will show the block size to different type of system nodes.

Systems	Block Size
Server, Desktop (24 Hrs Running) Tactical Platforms Indian Naval Ships Control Room	50 MB
GEO satellites AWACS Strategic Helicopters Small Naval Ship (Displacement>4000Tonnes)	20 MB
Server Desktop (non 24Hrs Running) LEO Satellites Small UAV Small tactical helicopters	10 MB
Laptop	5 MB
Cell Phone Attritable UAV Tactical Personal Systems	1 MB

Table 2: Proposed block size limit of different type of system nodes

Some of the characteristics of blockchain Main-Net are follows:

1) Private Blockchain:

The blockchain should be private mean who are authorized to use it can only use it. A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. Businesses who set up a private blockchain, will generally set up a permissioned network. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or permission to join. The access control mechanism could vary: existing participants could decide future entrants; a regulatory authority could issue licenses for participation; or a consortium could make the decisions instead. Once an entity has joined the network, it will play a role in maintaining the blockchain in a decentralized manner.[28]

The one of the example of private blockchain is “Hyperledger Framework”. Hyperledger is the umbrella open source project that the Linux Foundation has created and hosted since 2015. It aims at advancing and promoting cross-industry blockchain technologies to ensure accountability, transparency, and trust among business partners. The only framework of Hyperledger to provide privacy in terms of channel. So, a subset of members of the network can create channel among them and can maintain their separate ledger which is completely hidden from other members of the network. So, Hyperledger fabric may have multiple ledger (one ledger per channel) in order to maintain data privacy. [29]

Indian National Defence contractors can use such technology to create a private blockchain for their internal use and data safety.

2) Cyber Defense: Data integrity

Cyber defense is the most near-term, low-cost, high-payoff application of blockchain technology. As discussed earlier, cyber security relies on secrets and trust to maintain security, but neither can be assured. Blockchains operate independent of secrets and trust.Once Edward Snowden abused the trust of his administrator role to copy privileged files and then tampered with the audit logs that monitored his actions. He deleted a truth. Blockchains preserve facts in two ways. First, they ensure digital events are widely witnessed by sending them to other nodes on the blockchain network.

Blockchains also enhance cyber defense's perimeter security strategy, not by helping to hold up the walls, but by monitoring the walls and everything within them the growing complexity of modern systems, including weapon systems, make vulnerabilities both more likely and less detectable. "Instead of searching for vulnerabilities, equivalent to searching for a needle in a haystack, you can [monitor] every stalk of hay, every digital asset that constitutes the system you want to protect."[30]. Using blockchain, the configurations of every component in the system can be imaged, hashed, secured in the database, and continually monitored. Any unscheduled change to any configuration, no matter how small, can be detected almost instantly.

3) Supply chain management

There is growing anxiety about supply chain management for defense systems, which increasingly use commercial-off-the-shelf components for embedded software systems. The concern is that these components may contain deliberate vulnerabilities that could be exploited by an adversary at the time of his choosing.

Blockchains offer a solution that could establish the provenance of every circuit board, processor, and software component from "cradle to cockpit." The card design firm could use blockchains to log every design iteration of a circuit. Manufacturers could log every model and serial number of every card it produced. Finally, distributors could log the sale of batches of circuits to system integrators, who could log the allocation of circuits to specific aircraft assemblies, and so on. In this context, blockchains create a permanent records for the transfer of assets between owners, thereby establishing provenance.

Such a system also has clear benefits for both DOD and industry beyond a system's production phase. Many weapon systems are designed with service lives of 35 years or more. However, the computing technologies these systems use are rarely produced for more than a decade. As a result, replacing obsolete parts becomes more difficult with time

VII. Conclusion & Recommendation

The ability of the Indian Armed Forces to prevail in the highly contested environment of 2040 will be dictated by its ability to successfully conduct data-fighting operations. That is, protecting one's ability to generate, store, disseminate, process, analyze, and exploit information while interfering with the adversary's ability to do the same. Clearly, this requires a means of defending cyber-enabled systems from compromise. Yet contemporary cyber defense is faltering and is unlikely to improve given the evolving cyber threat.

This threat includes not only a growing array of malware and embedded computing devices, but also an adversary strategy that favors data manipulation over simple data theft. Thus, for the DRDO to prevail in data-fighting it needs to develop a model of cyber defense that addresses the failings of today's strategy and the future threat.

Blockchain technology offers such a model. Blockchains break with many of the flawed assumptions of traditional network security. First, blockchains are trustless; they assume compromise by both insiders and outsider. Second, blockchains are transparently secure; they do not rely on failure-prone secrets, but rather on a cryptographic data structure that provides a secure foundation on which to add additional security protocols.

The Indian Armed Forces should continue to explore blockchain technology for use in national defense applications. The following recommendations represent a path for this exploration.

1) Recommendation #1: Develop organic government expertise in blockchain technology. There is currently limited awareness or knowledge of blockchain technology within the Defence Experts and Indian Armed Forces and DRDO. To combat this, the DRDO with collaboration of Indian Armed Foces should establish a line of research to explore the potential blockchain technology. Research is needed to ensure that blockchains are sufficiently scalable, adaptable, and secure to support the Indian Armed Forces's broad array of missions in the air, Ground, Water, space, and cyber domains.
2) Recommendation #2: Partner with Private industry. The DOD should seek partnering opportunities with industry (Private and Public) to cooperatively and collaborative develop blockchain-based technologies for mutual benefit. The DOD and private industry share many common challenges, including the scourge of cybercrime and industrial espionage. Blockchain technology offers a new model of security and trust that could significantly mitigate a growing cyber threat.

REFERENCES

[1] Armed Forces vulnerable to cyber attacks, says Defence Minister, The Hindu, November 23, 2015 http://www.thehindubusinessline.com/info-tech/armedforces-vulnerable-to-cyber-attacks-says-defence-minister/article7909315.ece [last accessed February 17, 2016]
[2] Rica Bhattacharyya,72% Indian companies faced cyber attack in 2015: KPMG survey, The Economic Times, December 1, 2015 http://articles.economictimes.indiatimes.com/2015-12-01/news/68688315_1_cyber-risks-cyber-forensicskpmg-survey [last accessed February 17, 2016]
[3] Anirudh Bhattacharyya and Pramit Pal Chaudhuri, Was Beijing behind it and why?, Hindustan Times, April 12, 2010 http://www.hindustantimes.com/india/wasbeijing-behind-it-and-why/story-kR31Jmfg0b6sCEYxExDSJN.html [last accessed February 17, 2016]
[4] Yuthika Bhargava, India ranks second in cyber attacks through social media, The Hindu, April 22, 2015, http://www.thehindu.com/news/national/india-rankssecond-in-cyber-attacks-through-social-media/article7130961.ece [last accessed February 17, 2016]
[5] India a soft target for cyber criminals, says study, Business Standard, May 10, 2015, http://www.business-standard.com/article/current-affairs/india-a-soft-targetfor-cyber-criminals-symantec-115050900513_1.html [last accessed February 17, 2016]
[6] https://www.indiannavy.nic.in/sites/default/themes/indiannavy/images/pdf/resources/article_6.pdf
[7] G. O. Young, "Synthetic structure of industrial plastics," in Plastics, 2nd ed., vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
[8] W.-K. Chen, Linear Networks and Systems. Belmont, CA: Wadsworth, 1993, pp. 123–135.\
[9] https://securityaffairs.co/wordpress/45597/intelligence/china-hacked-us-defense-contractors.html
[10] https://economictimes.indiatimes.com/tech/internet/computers-of-armed-forces-and-drdo-hacked/articleshow/31550861.cms
[11] J. K. Author, "Name of paper," Abbrev. Title of Periodical, vol. x, no. x, pp. xxx-xxx, Abbrev. Month, year.
[12] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," IEEE Trans. Electron Devices, vol. ED-11, no. 1, pp. 34–39, Jan. 1959.
[13] E. P. Wigner, "Theory of traveling-wave optical laser," Phys. Rev., vol. 134, pp. A635–A646, Dec. 1965.
[14] E. H. Miller, "A note on reflector arrays," IEEE Trans. Antennas Propagat., to be published.
[15] https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[16] "Brief History of the Internet" (Internet Society, October 15, 2012),http://www.internetsociety.org/brief-history-internet.
[17] "A History of the ARPANET: The First Decade" (Defense Advanced Research Projects Agency, April 1, 1981).
[18] Antonopoulos, Mastering Bitcoin, chap. 1.
[19] Leslie Lamport, "The Byzantine Generals Problem," ACM Trans. Program. Lang. Syst. 4 (1982): 382–401, doi:10.1145/357172.357176.
[20] https://blockgeeks.com/guides/what-is-hashing/
[21] https://en.wikipedia.org/wiki/Mumbai
[22] http://www.hashemall.com/
[23] Antonopoulos, Mastering Bitcoin, chap. 7.
[24] Anthony Lewis, "A Gentle Introduction to Blockchain Technology," Bits on Blocks, September 9, 2015, http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/.
[25] Antonopoulos, Mastering Bitcoin, chap. 7.
[26] Paul Baran, "On Distributed Communications," Product Page, (1964),http://www.rand.org/pubs/research_memoranda/RM3420.html.
[27] "Beyond Distributed and Decentralized: What Is a Federated Network?," Institute of Network Cultures, accessed March 30,

2016,http://networkcultures.org/unlikeus/resources/articles/what-is-a-federated-network/.
[28] https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
[29] https://medium.com/@dhruvshah.navinchandra/unique-characteristics-of-hyperledger-frameworks-a9219ec3f012
[30] https://www.mycryptopedia.com/block-size-explained/

