International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I7P216

Volume 70 Issue 7, 147-157, July 2022

Original Article

Enhancing & Optimizing Security of IoT Systems using Different Components of Industry 4.0.

Rajat Verma[1], Namrata Dhanda[2], Vishal Nagar[3]

[1, *] *Department of CSE, ASET, Amity University, Lucknow, Uttar Pradesh, India.*
[2] *Department of CSE, ASET, Amity University, Lucknow, Uttar Pradesh, India.*
[3]*Department of CSE, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India.*

[1]rajatverma310795@gmail.com

Received: 06 May 2022 Revised: 29 June 2022 Accepted: 12 July 2022 Published: 20 July 2022

Abstract - *The technological ecosystem is developing at an exponential speed, causing the traditional security measures to fail and act as a ban on Modern Technologies. Likewise, Industry 4.0 requires Modern and SMART Solutions for better security and efficiency. The reason for considering this statement is that conventional security measures cannot continuously protect the rapid facts and figures generated. It is so because the techniques to attack, both active and passive, and the technologies being attacked are improving rapidly. By 2025, around 75 billion devices will be part of the connected system of the Internet of Things (IoT) that will surely generate vast data traversing worldwide, which needs to be secured and protected at any cost. Failure in doing so can lead to unfavourable situations. Since IoT belongs to Industry 4.0, a solution belonging to Industry 4.0 would be the best choice in solving the various challenges of IoT. This paper focuses on comparing diverse components of the fourth Industrial Revolution, namely Cloud Computing, BigData, Cognitive Domains, and Blockchain, to find the best parameter with a motive to secure IoT. Moreover, this paper also proposes a Hybrid Approach for optimizing and enhancing the security perspective of IoT.*

Keywords - *AI, Blockchain, Cloud, Cognitive, Privacy.*

1. Introduction

The Internet of Things (IoT) is an allied nexus, which consists of devices growing exponentially and is set to attain a target of 75 billion connected devices by 2025 [1]. An enormous set of devices means a huge set of data that must be protected [2]. Conventional techniques currently protecting IoT are outdated and require Modern & SMART solutions [3]. IoT belongs to Industry 4.0. [2011] that includes the involvement of Cyber-Physical Systems (Working on Algorithms). Previous Industrial Revolutions that are 1.0. [1765], 2.0. [1870], 3.0. [1969], included Man Power to Machines (Industrial), Electrical Technology (Technological), and Computers (Digital Revolution), respectively [4]. Different components of this industry involve Cloud Computing, Cognitive Computing, Blockchain, Cyber-Physical Systems, etc. The initial term, i.e., Cloud Computing, considers any division of hosted services through cyberspace, i.e., the Internet. The three important pillars of the Cloud are IaaS, PaaS & SaaS [5]. In Modern Scenarios, various other services also act as the cloud's pillars. For instance, Backend and Analytics are performing as a Service and are abbreviated as BaaS and AaaS, respectively [6-7]. The Next parameter, i.e., Cognitive Computing, involves the usage of models (computerized) to imitate the compounded mental process of Humans [8]. Specifically, Cognitive Computing imitates the personality of a Human-Being. It improves the decision-making process by following the principles of Machine Learning and its sub-classifications [9-10]. The Next Measure of Industry 4.0 is blockchain, a Network of Peer-to-Peer devices [11]. Blockchain works on three basic principles: Immutability, Decentralization, and Transparency. The Last one is the Cyber-Physical Systems which includes the working of Intelligent Systems, which are checked by Algorithmic Rules which are pre-defined [12]. In Artificial Intelligence (AI), an Intelligent Agent has two major characteristics: a System that imitates Humans and a System that acts and Thinks rationally [13]. This Paper Focuses on Finding the Best Security Solution for IoT from Industry 4.0. All these Parameters of the Industry 4.0 are illustrated and compared in the next sub-sections for an appropriate consideration of the subject.

2. Components of Industry 4.0.

Industry 4.0. is an extensive transformation in automation involving many technologies that can act as a primary solution to many security issues of the Internet of Things. The Research Background of all these solutions is depicted here in this section.

2.1. Internet of Things (IoT)

The Internet of Things is a web of connected nodes for sharing facts and records through cyberspace, i.e., the Internet [14]. It is a system that works with electronic objects in this technological world [11]. It can involve Human-Beings or perform functions without the intervention of Human-Beings. The Journey of IoT began with the invention of a smart toaster. Since then, the popularity of IoT has reached many milestones.

By 2025, around 75 billion nodes are considered a constituent of an allied nexus of IoT [1]. With this massive increment in the number of devices, the security, privacy, and interoperability objectives will be in concern that needs to be secured [11]. The Diverse Issues of IoT are highlighted in Table 1 for easy understanding [11, 15-19].

Table 1. Shows the Issues in IoT

S.No	Security Concerns in IoT
1	Centralization: Single Point of Failure
2	Fabricated Data
3	Perception Layer: Multiple Terminals
4	User Data Privacy, Data Encryption
5	Data Attacks
6	Concerns About Fairness of Data Collection and Use
7	Concerns About Transparency, Expression & Enforcement
8	Tampering
9	Outdated Security

The attacks highlighted in Table 1 need to be attended to enhance and optimize the security standard of the conventional IoT. The different strategies of Industry 4.0 are well depicted and compared to find the best solution for issues of IoT.

2.2. Cloud Computing

The delivery of diverse services or resources through the Internet corresponds to the functioning of the cloud. The cloud is the ultimate Centralized Processing System [20], so it cannot solve the centralization concern of IoT alone. Although, by incorporating Edge Computing into Cloud, Decentralization can be implemented [21]. It will deal with a major drawback of complexity as decentralization will be an amalgamated version of two technologies. Also, the cloud follows the private and public existence of facts and figures. It means that there is no certainty in keeping the data transparent. Hence, it also cannot tackle the transparency issue of IoT. The cloud focuses on conventional databases that only support the facts that resided in the machines involving participants. It signifies that the cloud can be corruptible and unreliable, which indicates that it cannot solve the Tampering aspect of IoT. The following Table 2 shows IoT's drawbacks tackled by the cloud.

Table 2. Shows Issues of IoT tackled by cloud

Issue of IoT	Cloud	Solution
Centralization	Follows Centralization	Not Solved
Transparency	Either Private or Public	Partially
Mutability	Corruptible	Not Solved
Fabricated Data & Tampering	Corruptible	Not Solved

Many pillars of Cloud Computing (Traditional and Modern) are depicted below for quick and easy grasp.

With Modern Enhancements in Technology, many new Pillars are also added to the conventional ones. They are mentioned below.

1) Platform as a Service: It is abbreviated as PaaS. In this scenario, the cloud provider gives the complete platform to use and maintains all the components of the required architecture. The Provider takes care of Pre-defined Tools, Servers, Virtual Machines, etc. App Engine from Google Cloud is a Very Popular Example in this category [22].
2) Software as a Service: It is abbreviated as SaaS. Here, the cloud provider focuses on Application Codes, Databases in the form of machines [23]. A few Popular Examples in this category are Fresh Desk and Self-Service Solution.
3) Infrastructure as a Service: It is abbreviated as IaaS. Over here, the Infrastructure and computer architecture is provided. A Very Popular Example in this category is AWS from Amazon [24].
4) Data as a Service: For Better insights, a variety of pre-calculated and pre-aggregated data is required. The benefit of this will be a better decision process. A Very Popular Example in this category is Mongo DB. [25]. The cloud provides Data Storage and Processing along with Integration in this.
5) Database as a Service: It is facilitated by Private and Public Cloud Providers to provide the functions of a database. The Scale grid for MySQL is a Very Popular Example in this category [26].
6) Desktop as a Service: It is a subscription-based model, considering a Virtual Desktop that can be hosted over the cloud platform. A Very Popular Example in this category is V2 Cloud. It is hosted on-premises [27].
7) Function as a Service: It provides a server-less architecture. AWS Lambda, developed by Amazon, uses this functionality. Azure also supports this. [28]
8) Backend as a Service: The Vendor provides this as a service that is different from the Front End. Push Notifications, Cloud Storage, Database Management, and User-Authentication come under this category. [29]

2.3. Cognitive Computing

Cognitive computing can imitate the compounded mental process of Humans in a computerized learning model. It is a core component of Industry 4.0. It does so by using the algorithmic rules of self-learning that use pattern recognition, data mining, and NLP. Data in IoT can also use Cognitive to imitate human behaviour of how a user operates an IoT device. It uses the advanced level of Artificial Intelligence (AI) to create a computer that thinks. It is not a security technique, but it can be added with some modern and SMART solutions to give IoT the security that IoT is dreaming of. One such technology is blockchain [11], which could handle the security concerns of IoT. So, in totality, the amalgamated version of Blockchain and Cognitive can be a boon for IoT Security. Finance is one of the first industries to use this approach [30-31]. The importance of blockchain is highlighted in the next sub-section.

2.4. Blockchain

American Cryptographer David Chaum initiated the initial blockchain-like protocol in his dissertation in 1982 [32]. Then in 1991, it was further evolved by W. Scott Stornetta and Stuart Haber [33]. Then after 17 years, i.e., in 2008, the first conceptualization of blockchain came up behind the renowned cryptocurrency Bitcoin and was called by a false identity named "Satoshi Nakamoto" [34]. Blockchain is developed in three phases, the first part started in 2008 and lasted 5 years till 2013, and this phase was known as Bitcoin Emergence as Blockchain 1.0. Then after the first phase, for the next two years, i.e., till 2015, the next phase was called Ethereum Development and was represented by Blockchain 2.0. The application phase represents the last 7 years of blockchain as Blockchain 3.0 [35]. Cardano represented it. Blockchain is a decentralized network technology that includes blocks connected using cryptographic hash values. Block is a building constituent of a blockchain, which contains few entities for its proper functioning. The composition of a block is illustrated in Figure 1.

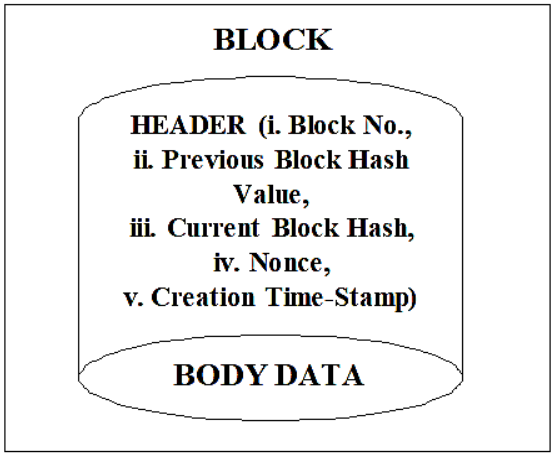

Fig. 1 Structure of a Block (inc. Header & Body Data) [11].

In Figure 1, the sub-parts of a block are highlighted that contain entities in two halves. The upper one is known as the Header, while the lower entity is called body data. The Header section is quite important as it contains more sub-entities such as the position of the constituent node, the preceding hash digest concerning the next node and secured hash value of the current block, a security parameter termed Nonce, and the timestamp of the creation of the block [36].

When the blocks combine, they form a chain, which is termed a blockchain. Blockchain follows the principle of the longest chain, originally termed a Main-chain. If the Blocks belong to the main chain, they are valid; if not, they have termed orphan blocks [37]. The concept of a blockchain with both valid and orphan blocks is highlighted in Figure 2.

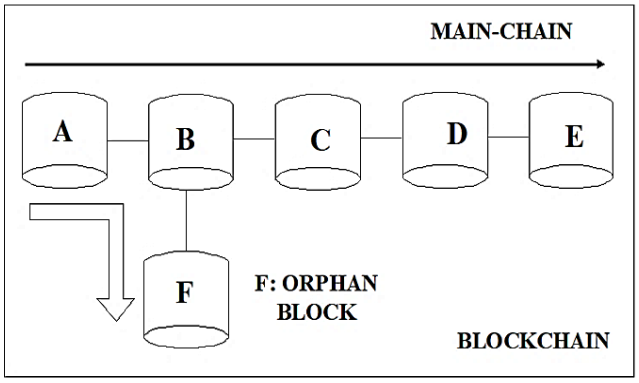

Fig. 2 Blockchain Layout

In Figure 2, a total of 6 systems are there, where two chains are highlighted. One from A-B-C-D-E and the second from A-B-F. The chain concerning 5 nodes, i.e., from A to E, is the main chain, and the second chain concerning three nodes, i.e., from A to F, represents the orphan chain. Since F is not part of the main chain, it will be termed an orphan block. Considering it is working, the first block represented by A has a special name called the Genesis Block [38]. A will not have a previous hash, as no block exists before A. The Next Block B will have all the entities as depicted traditionally. The previous block hash of B will be identical to the current hash of A. It is quintessential as the blocks would not be connected without it. Blockchain has three salient attributes: Immutability, transparency, and decentralization [39]. As the cloud is corruptible and data can be fabricated in Cloud, Blockchain, with its characteristics, tackles these issues efficiently. The concept of fabricated data of IoT, thus the following mutability, and how it can be dealt with blockchain is represented in Figure 3.

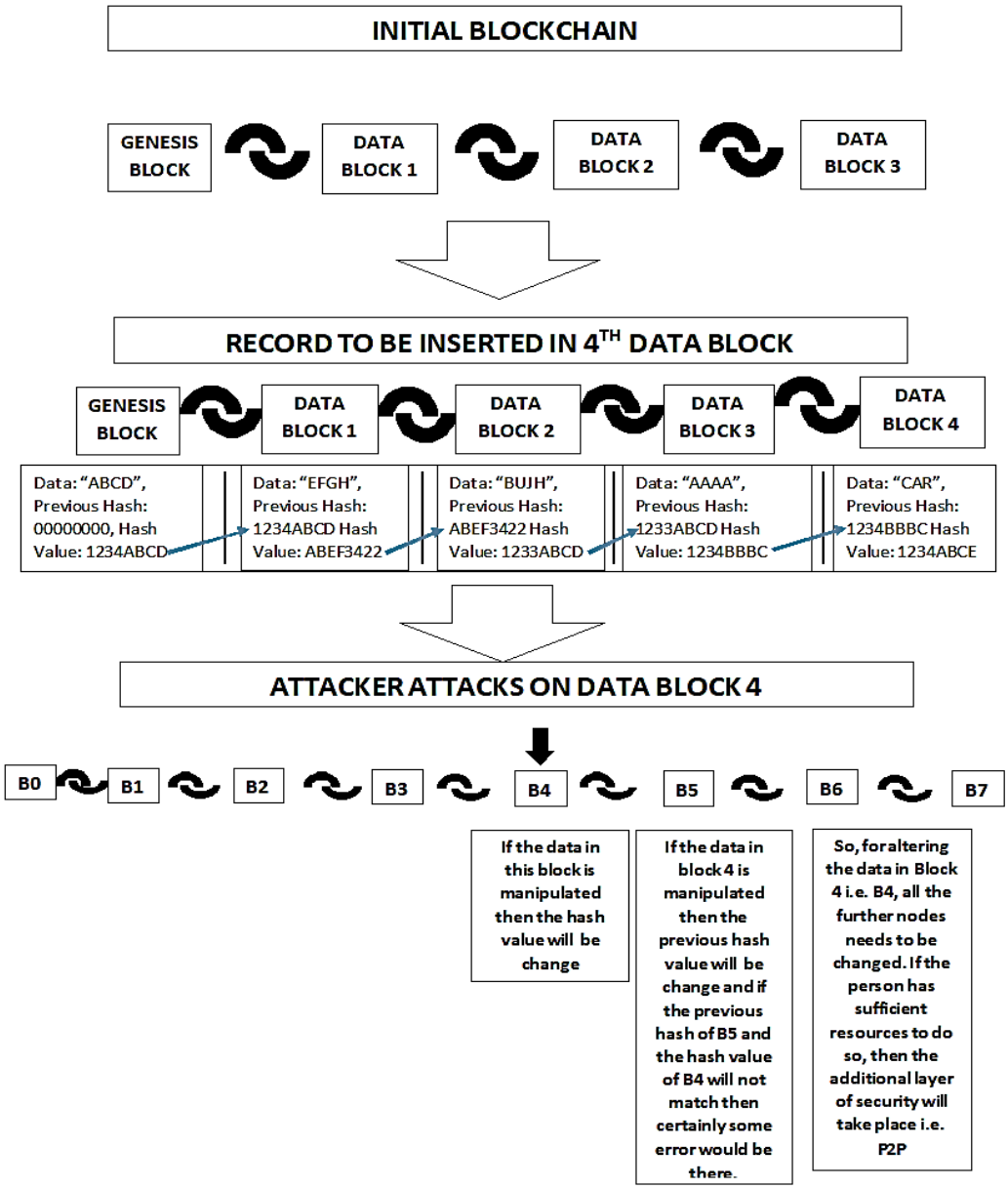

Fig. 3 Immutability with Blockchain, thus minimizing Fabricated Data/Tampering

In Figure 3, the concept of Immutability is highlighted. To understand this Figure, let us suppose that some data is available at the fourth node of the chain. A cyberespionage tries to damage the fourth block of the blockchain and attempts to manipulate the data available in it; as the attacker does this, the hash value of the concerned node is altered. To maintain the equality of the previous hash of the succeeding block (i.e., fifth) and the current hash of the fourth node, the cyber attacker has to alter the data in the next block (fifth) accordingly. Suppose the attacker does so; a similar scenario will happen with the fifth and the sixth node, and it will go till the termination point. After this, if the culprit alters complete data in one chain. To follow the decentralization process, the interloper has to manipulate the entire contents available in the network. Even if the interloper has vast resources, tampering with the entire contents is somehow impossible [11].

By this, blockchain eliminates the problem of fabricated data and tampering in IoT. Figure 4 depicts the decentralization characteristic of Blockchain in IoT, thus eliminating the problem of the centralization of IoT.

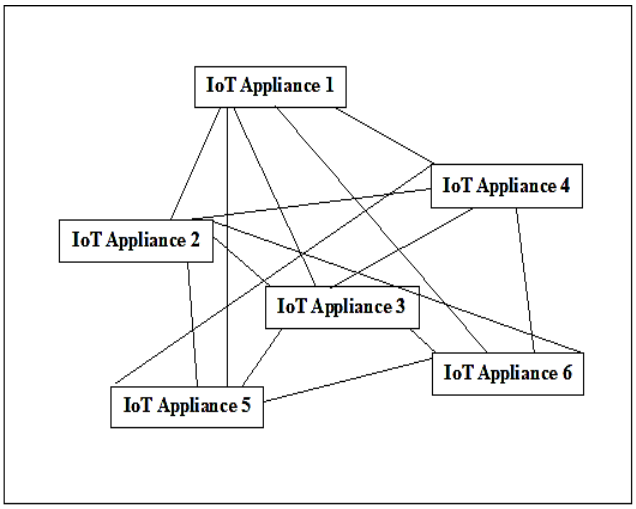

Fig. 4 Decentralized IoT Network

In Figure 4, a decentralized network of six IoT appliances is considered. However, it can be considered up to n nodes depending on the network's capacity. With this network, it can eradicate the single point of failure and error.

Since blockchain protects data from Tampering, it can minimize data inconsistency, breaches, and unauthorized access [40] that the cloud cannot prevent. It follows the ECDSA, a combined form of Elliptic-Curve Cryptographical Technique and Digital Signature for more security. A very popular algorithm for the security of IoT is RSA Algorithm.

RSA stands for Rivest-Shamir-Adleman Encryption. Traditionally, RSA is used to secure the alliance between the Web-Browser and the IoT Platform. It was introduced in 1977, so it has to be upgraded with time. On the other hand, ECC was introduced in 1985 [41]. ECC provides the same amount of security with less key size. Another advantage of ECC over RSA is scalability as well as performance. With a shorter number of keys, a lesser load is required for the network and computation [42]. With this, blockchain is one step ahead with the security of IoT devices. The key size of the RSA and ECC Algorithm is compared in Figure 5.

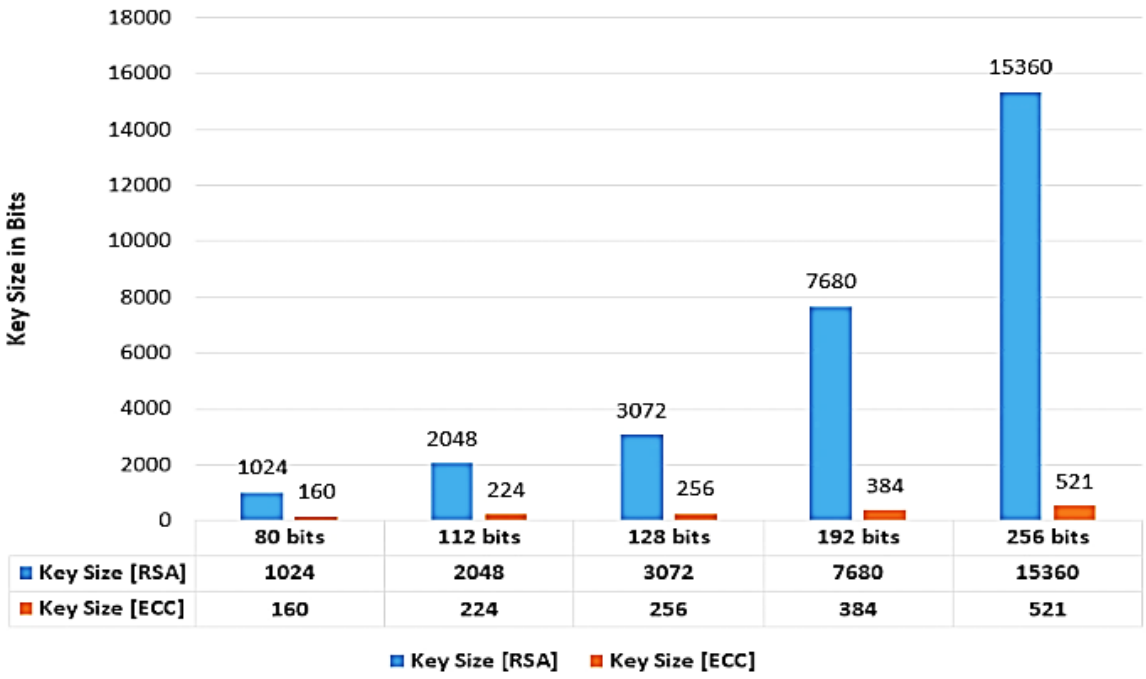

Fig. 5 Key Size of RSA Algorithm V/S Key Size of ECC Algorithm

For securing the operations and encryption purposes, blockchain uses Secure Hashing Algorithms, particularly 256, which gives the persistent output of 64-hexadecimal entities [43]. So, an amalgamated version of SHA-256 & ECC is used in blockchain that is suitable for enhancing the IoT Security spectrum. Various Solutions of IoT solutions through blockchain are below in Table 3 for easy understanding.

Table 3. Issues of IoT tackled by blockchain

Issue of IoT	Blockchain	Solution Obtained
Centralization	Follows Decentralization	Yes
No Transparency	Follows Transparency	Yes
Mutability	Follows Immutability	Yes
Fabricated Data/Tampering	Follows Immutability	Yes
Outdated Security	ECC	Enhanced Security
User Data Privacy, Data Encryption	ECC+ SHA-256	Yes
Data Attacks	Follows Immutability, Decentralization	Minimized the risk of Data Attacks
Fairness	Consensus Algorithms	Yes
Multiple Terminals	SHA	Solved
Trust	Follows Immutability, Decentralization, Transparency	Enhanced Trust

2.5. BigData

BigData is a constituent element of the fourth industry of the Industrial Revolution. The data generated by IoT is big data that is highly inaccurate, inconsistent, and incomplete. The data in BigData persist seven characteristics [44-47]:

1. Volume: By 2025, the data volume of IoT will be around 79.5 zettabytes (ZBs). [44]

2. Velocity: It indicates the rate at which the facts and figures are created. If the volume of IoT data reaches 79.5 ZBs [44], then a high data generation must persist.

3. Variety: The data IoT generates has variety, consisting of structured, semi-structured, and unstructured data.

4. Variability: The data generated in IoT is mutable, which shows the measure of variability.

5. Veracity: The veracity in IoT is average. Since IoT generates inaccurate and inconsistent data, enhancing integrity would be a measure to look out for.

6. Value: Worldwide IoT data has a value of $1.1 trillion by the year 2025 [45-46]

7. Visibility: With this characteristic feature, IoT visibility can map and correlate the customer journey in IoT [47].

For Protecting this IoT BigData, Blockchain will be a suitable technology [11, 48].

3. Comparison Of Cloud, Cognitive Computing, Blockchain, Bigdata Concerning IoT Dream Security

The following Table 4 compares different elements of Industry 4.0 to strengthen the security and privacy perspective of IoT.

Table 4. Comparison of Diverse Industry 4.0. Techniques

Issue of IoT	Cloud	Cognitive Computing	Blockchain	Big Data
Centralization	Follows Centralization	Not a security Technique, but if amalgamated with blockchain, then the amalgamated version of Cognitive and Blockchain could achieve IoT Dream Security.	Follows Decentralization	Not a security Technique, but if amalgamated with blockchain, then the amalgamated version of BigData and Blockchain could achieve Good IoT Security.
No Transparency	Partial Transparency		Complete Transparency	
Mutability	Mutable		Immutable	
Fabricated Data/Tampering	High Possibility		Not Possible	
Outdated Security	RSA/AES		ECC, Enhanced Security	
User Data Privacy, Data Encryption	Not Secured, as it is mutable, weak standards.		Highly Secured	
Data Attacks	Corruptible, Hence Possible.		Not Corruptible, Hence Not Possible	
Fairness	Partial		Complete	
Multiple Terminals	Partially Solves		Secured through Consensus.	
Trust	Not Achievable		Achievable, Enhanced Trust	

4. Proposed Framework For Enhancing Security of IoT

In the previous sections, it was depicted in what manner blockchain will eradicate IoT issues. In this section, a proposed framework shows the amalgamated blockchain version with different aspects of Industry 4.0. With modifications and after testing, if implemented commercially, it can boost the security parameter of IoT. The proposed approach is highlighted in Figure 6.

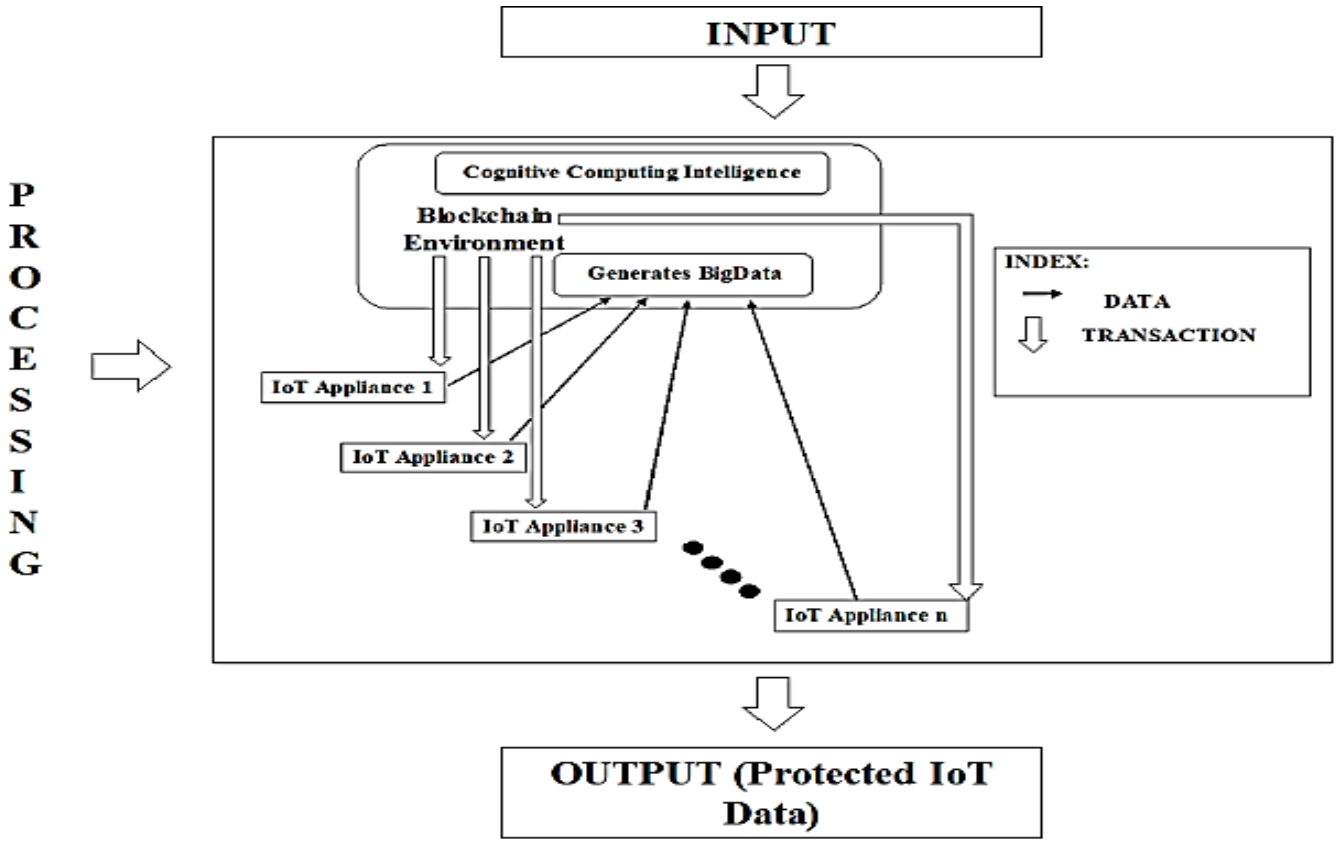

Fig. 6 Proposed Hybrid Framework for enhancing security in IoT

In Figure 6, the proposed framework is highlighted, which works in the following manner. The input node is initially present, showing how the IoT peer devices provide the data signals. The next phase, i.e., the Processing Phase, is the area where the security of IoT data is enhanced. In the processing phase, the IoT will generate a voluminous amount of information, typically called Big Data, since the BigData node is protected by blockchain with its three characteristic features, i.e., Decentralization, Immutability, and Transparency. In addition, Cognitive Computing measures will provide self-learning capabilities with the help of data mining, Natural Language Processing, Machine Learning, etc. [49]. With this self-protected and self-learned mechanism, protected IoT data will be generated. The support of transactions is already there to create a Merkle tree of the hashes, thus enhancing security. The result of it will be Protected IoT Data. The Protected IoT Data will improve security, such as enhanced trust and integrity.

5. Comparison of ECC & RSA

in Section 2.4, ECC performs better than the traditional algorithm of IoT. The Length of the key in ECC is much more compact and minute than the Key-Length of RSA. In this Section, the Key-Length along with the Key-Generation Time of ECC and RSA are compared where ECC, which is used in blockchain, is a winner. The detailed spectrum is shown below in Table 5.

Table 5. Key Length & Key Generation Time Comparison of ECC & RSA

S.No.	Key-Generation (Nature: Approximate)			
	Key-Length		Time	
	ECC	RSA	ECC	RSA
1.	163 [bits]	1024 [bits]	0.08 [Seconds]	0.16 [Seconds]
2.	233 [bits]	2240 [bits]	0.18 [Seconds]	7.47 [Seconds]
3.	283 [bits]	3072 [bits]	0.27 [Seconds]	9.80 [Seconds]
4.	409 [bits]	7680 [bits]	0.64 [Seconds]	133.90 [Seconds]
5.	571 [bits]	15360 [bits]	1.44 [Seconds]	679.06 [Seconds]

6. Results and Discussion

The IoT Technology is developing at a lightning-fast speed whose details are already depicted in Bigdata & IoT Section. The immense number of connected IoT devices, i.e., around 75 billion by the year 2025 [1], will certainly generate a gigantic spectrum of security and privacy concerns highlighted in this paper in Table 1. One point that

can be convincingly obtained from the above textual matter is that many components are available in Industry 4.0, but the "Blockchain" Parameter is the next big thing. The Blockchain approaches to IoT issues will certainly enhance the Security Perspective of IoT. Blockchain has gained optimal popularity from the time it was used behind Bitcoin.

Similarly, it could be amalgamated commercially with IoT to enhance security and efficiency. Cognitive cannot achieve security alone, but the blended approach with blockchain could achieve dream IoT security, highlighted in the Cognitive Computing Section and Proposed Framework Section and Table 4. The detailed solution of blockchain for diverse problems of IoT is highlighted in Blockchain Section and Tables 3 and 4. Proposed Framework Section shows the hybrid proposed framework for security enhancement of IoT. The detailed cloud computing scenario that can tackle IoT issues but not efficiently is also highlighted in Table 2. The contrast between ECC and its predecessor, i.e., RSA, is also illustrated in Fig 5, Table 5.

7. Conclusion & Future Scope

The current scenario of the technological world has witnessed the omnipresent nature of the Internet of Things. The data known as facts and figures is particularly the primary cause of the popularity of IoT. Because of this popularity, IoT has become omnipresent. With the evolved quantity of data, there will be a greater threat to the security aspect of the IoT Spectrum. In Industry 4.0, there are various measures. Still, one technology is victorious among all, i.e., the combined approach of Blockchain and Cognitive Computing which is highlighted in an elaborative way in this paper. A detailed review of Cloud Computing, Cognitive Computing, the Internet of Things, Blockchain, and BigData is also presented here. The Amalgamated Implementation of Blockchain with Cognitive Intelligence can be performed to improve the privacy and security spectrum of the conventional IoT. It will have diverse use cases of IoT [50].

Similarly, the researcher will continue working in the domain of IoT & Blockchain.

References

[1] Bera A , "Insightful Internet of things statistics (Infographic)," White Paper. Retrieved from https://safeatlast.co/blog/iot-statistics/#gref

[2] Verma, R., Dhanda, N., Nagar, V, " Towards a Secured IoT Communication: A Blockchain Implementation Through APIs," In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems*, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_53.

[3] Ali Haider Shamsan, Arman Rasool Faridi, "A Novel SDNFV IoT Architecture Leveraging Softwarization Technology Services to Alleviate IoT Network Resource Restrictions, " *International Journal of Engineering Trends and Technology*, vol.70, no.2, pp. 1-10, 2022.

[4] Popkova, E. G., Ragulina, Y. V., & Bogoviz, A. V, "Fundamental differences of transition to industry 4.0 from previous industrial revolutions," *In Industry 4.0: Industrial Revolution of the 21st Century* , pp. 21-29, 2019. Springer, Cham.

[5] Walterbusch, M., Martens, B., & Teuteberg, F, "Evaluating cloud computing services from a total cost of ownership perspective," *Management Research Review*, 2013.

[6] Dahunsi, F. M., Idogun, J., & Olawumi, A, "Commercial Cloud Services for a Robust Mobile Application Backend Data Storage," *Indonesian Journal of Computing, Engineering and Design* (IJoCED), vol.3, no.1, pp.31-45, 2021.

[7] Lehner, W., & Sattler, K. U, "Database as a service (DBaaS)," *In 2010 IEEE 26th International Conference on Data Engineering*, (ICDE 2010) pp. 1216-1217, 2010. IEEE.

[8] Megha, C. R., Madhura, A., & Sneha, Y. S, "Cognitive computing and its applications," In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), pp.1168-1172, 2017. IEEE.

[9] Preece, A., Cerutti, F., Braines, D., Chakraborty, S., & Srivastava, M, " Cognitive computing for coalition situational understanding," *In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation* (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) , pp. 1-6, 2017.EEE.

[10] Huang, K., Hussain, A., Wang, Q. F., & Zhang, R. (Eds.), " Deep learning: fundamentals, theory and applications," Vol. 2, 2019. Springer.

[11] Verma R., Dhanda N., Nagar V, "Security Concerns in IoT Systems and Its Blockchain Solutions," In: Tavares J.M.R.S., Dutta P., Dutta S., Samanta D. (eds) Cyber Intelligence and Information Retrieval. *Lecture Notes in Networks and Systems*, vol 291, 2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-4284-5_42.

[12] Verma, R., Dhanda, N., Nagar, V, " Application of Truffle Suite in a Blockchain Environment, " In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*. Lecture Notes in Networks and Systems, vol 421, 2023. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_54.

[13] Geetha, R., & Bhanu, S. R. D, " Recruitment through artificial intelligence: a conceptual study," *International Journal of Mechanical Engineering and Technology*, vol.9, no.7, pp. 63-70, 2018.

[14] A. Srikrishnan, Dr. Arun Raaza, Dr. B. Ebenezer Abishek, " Internet of Things (Iot) Network Security using Quantum Key Distribution Algorithm, " *International Journal of Engineering Trends and Technology*, vol.70, no.2, pp.19-23, 2022.

[15] Sengupta, J., Ruj, S., & Bit, S. D, " A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol.149, pp.102481, 2020.

[16] Kumar, N. M., & Mallick, P. K, "Blockchain technology for security issues and challenges in IoT, " Procedia Computer Science,vol. 132, pp.1815-1823, 2018.

[17] Verma, R., Dhanda, N., & Nagar, V," Addressing the issues & challenges of internet of things using blockchain technology," *International Journal of Advanced Science and Technology*, vol.29, pp.10074–10082, 2020.

[18] Aqeel-ur-Rehman, S. U. R., Khan, I. U., Moiz, M., & Hasan, S, "Security and privacy issues in IoT," *International Journal of Communication Networks and Information Security* (IJCNIS), vol.8, no.3, pp.147-157, 2016.

[19] Hameed, A., & Alomary, A ,"Security issues in IoT: A survey," *In 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies* (3ICT) , pp.1-5, 2019. IEEE.

[20] Wu, J., Zhang, Z., Hong, Y., & Wen, Y, " Cloud radio access network (C-RAN): a primer, " *IEEE network*, vol.29, no.1, pp.35-41, 2015.

[21] Georgakopoulos, D., Jayaraman, P. P., Fazia, M., Villari, M., & Ranjan, R, "Internet of Things and edge cloud computing roadmap for manufacturing," *IEEE Cloud Computing*, vol.3, no.4, pp.66-73, 2016.

[22] Gai, K., & Steenkamp, A ,"A feasibility study of Platform-as-a-Service using cloud computing for a global service organization," *Journal of Information Systems Applied Research*, vol.7, no.3, pp.28, 2014.

[23] Lakshmisri, , " Software as a service in cloud computing," *International Journal of Creative Research Thoughts* (IJCRT), ISSN, vol. 2320no, 2822, pp.182-186.

[24] Serrano, N., Gallardo, G., & Hernantes, "J. Infrastructure as a service and cloud technologies," *IEEE Software*, vol.32, no.2, pp. 30-36, 2015.

[25] Lu, C. W., Hsieh, C. M., Chang, C. H., & Yang, C. T, " An improvement to data service in cloud computing with content sensitive transaction analysis and adaptation," *In 2013 IEEE 37th Annual Computer Software and Applications Conference Workshops*, pp.463-468, 2013. IEEE.

[26] Curino, C., Jones, E. P., Popa, R. A., Malviya, N., Wu, E., Madden, S., & Zeldovich, N, " Relational cloud: A database-as-a-service for the cloud, " 2011.

[27] Shu, S., Shen, X., Zhu, Y., Huang, T., Yan, S., & Li, S, "Prototyping efficient desktop-as-a-service for fpga based cloud computing architecture," *In 2012 IEEE Fifth International Conference on Cloud Computing* , IEEE, pp.702-709, 2012.

[28] Van Eyk, E., Iosup, A., Abad, C. L., Grohmann, J., & Eismann, S. "A SPEC RG cloud group's vision on the performance challenges of FaaS cloud architectures, " *In Companion of the 2018 ACM/SPEC International Conference on Performance Engineering*, pp. 21-24, 2018.

[29] Costa, I., Araujo, J., Dantas, J., Campos, E., Silva, F. A., & Maciel, P, " Availability Evaluation and Sensitivity Analysis of a Mobile Backend-as-a-service Platform," *Quality and Reliability Engineering International*, vol.32, no.7, pp. 2191-2205, 2016.

[30] Chen, Y., & Bellavitis, C, " Blockchain disruption and decentralized finance: The rise of decentralized business models, " *Journal of Business Venturing Insights*, vol.13, pp.e00151, 2020.

[31] Garzik, J., & Donnelly, J. C. "Blockchain 101: an introduction to the future, In Handbook of Blockchain, Digital Finance, and Inclusion," Vol. 2, pp.79-186,2018. Academic Press.

[32] Kekulandara, M, "A Blockchain-based Auditable and Secure Voting System (Doctoral dissertation, University of Rhode Island) ," 2020.

[33] Panda, S. K., Elngar, A. A., Balas, V. E., & Kayed, M. (Eds.), "Bitcoin and Blockchain: History and Current Applications," *CRC Press* , 2020.

[34] Nakamoto, S, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, pp. 21260, 2008.

[35] Mukherjee, P., & Pradhan, C, " Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology," In Blockchain Technology: Applications and Challenges, pp. 29-49 , 2021. *Springer, Cham*.

[36] Zhu, L., Gai, K., & Li, M ," Blockchain Technology in Internet of Things," Germany: *Springer*, pp.1-143, 2019..

[37] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C. A., Nyang, D., & Mohaisen, A, "Overview of attack surfaces in blockchain," *Blockchain for distributed systems security*, pp. 51-66, 2019.

[38] Rajesh Kumar .M, Venkatesh .J, Zubair Rahman .A. M. J. Md, " Feature Centric Data Augmentation Model-Based Mobile Commerce for Efficient Retail Growth using BlockChain," *International Journal of Engineering Trends and Technology*, vol. 70, no.3, pp. 179-184, 2022. https://doi.org/10.14445/22315381/IJETT-V70I3P220.

[39] Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R ," Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," *In the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany*) , IEEE, pp.1-4, 2018.

[40] Shaverdian, P, " Start With Trust: Utilizing Blockchain to Resolve the Third-Party Data Breach Problem," *UCLA L*. Rev., pp.66, pp. 1242, 2019.

[41] Lopez, J., & Dahab, R, "An overview of elliptic curve cryptography," 2000.

[42] Gupta, V., Gupta, S., Chang, S., & Stebila, D. "Performance analysis of elliptic curve cryptography for SSL," *In Proceedings of the 1st ACM workshop on Wireless security*, pp. 87-94, 2000.

[43] Verma, R., Dhanda, N., Nagar, V, " Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms, " In: Kaiser, M.S., Bandyopadhyay, A., Ray, K., Singh, R., Nagar, V. (eds) *Proceedings of Trends in Electronics and Health Informatics*. Lecture Notes in Networks and Systems, Springer, Singapore, vol.376 , 2022. https://doi.org/10.1007/978-981-16-8826-3_44.

[44] Data volume of internet of things (IoT) connections worldwide in 2019 and 2025(in zettabytes). Retrieved from https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/#:~:text=Data%20volume%20of%20IoT%20connected%20devices%20worldwide%202019%20and%202025&text=The%20statistic%20shows%20the%20overall,reach%2079.4%20zettabytes%20(ZBs)

[45] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D, "Unlocking the Potential of the Internet of Things", *McKinsey Global Institute*, vol.1, 2015.

[46] Castillo O'Sullivan, A., & Thierer, A. D, "Projecting the growth and economic impact of the internet of things," Available at SSRN 2618794, 2015.

[47] Ng, I. C., & Wakenshaw, S. Y, "The Internet-of-Things: Review and research directions," *International Journal of Research in Marketing*, vol.34, no.1, pp. 3-21, 2017.

[48] Karafiloski, E., & Mishev, A , "Blockchain solutions for big data challenges: A literature review," *In IEEE EUROCON 2017-17th International Conference on Smart Technologies* , IEEE. pp. 763-768, 2017

[49] Goodfellow, I., Bengio, Y., & Courville, A,"Machine learning basics," *Deep learning*, vol.1, no.7, pp.98-164, 2016.

[50] P.Maungmeesri, K. Kantananon, B. Maungmeesri, D. Maneetham, " The Innovation for Smart Patient Screening Platform via IoT System," *International Journal of Engineering Trends and Technology*, vol.70, no.2, pp.192-200, 2022.