DOI : https://doi.org/10.53555/nncse.v9i7.1844 Publication URL:https://nnpub.org/index.php/CSE/article/view/1844

ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN TECHNOLOGY FOR SECURE DATA AND PRIVACY

Shaikh Abdul Hannan*

**Assistant Professor, Department of Computer Science and Information Technology, AlBaha University, AlBaha, Kingdom of Saudi Arabia.*

Corresponding Author:

Abstract

Data, which is then processed in order to extract the desirable characteristics, serves as the input for a number of different AI algorithms. However, the facts that can be found on the internet are incredible and tough to authenticate. Given the complexity of the internet, it is quite challenging to validate the data for the consumers. Consequently, in this research, we suggested using SecNet as a solution. An architecture that assists in the protection of data storage, the processing of data, and the sharing of large-scale Internet settings is known as SecNet. The primary objective of this architecture is to enhance the performance of artificial intelligence algorithms across a variety of data sources in order to provide a cyberspace that is more safe and to make use of actual big data. This architecture combines and supplies the following three primary components: 1) The trading of data based on a blockchain is carried out with the ownership of the data being assured. This enables the interchange of accurate data in a wide-ranging environment and contributes to the formation of actual big data. 2) The protection of an AI-based secure computing platform that is powered by artificial intelligence to develop more astute security standards and contribute to the establishment of a cyberspace that is more reliable. 3) The trustworthy value-sharing Security Service buy Mechanism gives participants a fantastic opportunity to gain Economic Rewards for the provision of data or services, which makes data sharing easier and ultimately leads to improved AI performance .

Keywords: *Artificial, Intelligence, Blockchain Technology*, Data Security, SecNet, Privacy.

INTRODUCTION

Not only is there a growing trend toward the incorporation of cyberphysical social (CPS) systems into the digital Internet, but there is also a growing trend toward the incorporation of these systems into an information society that adheres to stringent norms and protocols. This trend is the result of advancements in information technology.[1] In a society as information-oriented as our own, data belongs to the owner, and the owner must have complete control over how the data is used, which is not always the case. However, in our culture, this is not always the case. Since data is most likely the crude oil of the information age, virtually every big organisation is working hard to collect as much data as they possibly can in order to increase their chances of being competitive in the future. These massive corporations embed sensors into their goods, which subsequently enhance the amount of personal data that may be collected, such as a user's location, their internet search activity, their phone conversations, and their preferences.[2] These sensors pick up this information explicitly as well as indirectly. This puts the data owner's right to personal privacy in serious jeopardy and poses a major risk. In addition, the owner has no say in the manner in which these data are utilised because there is currently no reliable mechanism to record either the manner in which the data are used or the individuals who are using them. Because of this, the owner is placed in a precarious situation. As a consequence of this, there are not many ways to catch a data abuser or tracker who is acting in a way that is contrary to the terms of service for this data. Or an admonition. Because of this, you won't be able to effectively manage your data, which will make it exceedingly difficult for you to deal with the potential risks related with the data you've obtained. For example, if data is collected by a third party (such as a large organisation), then that data is not available, and individuals are unable to appreciate or manage the risks associated with the data they are obtaining since those risks are not under their control. [3] On the other hand, there is no ongoing record of how the data are used, which raises the risk that the data may be misutilized. Moreover, there is no way to tell whether or not the data have been altered. If there is a quick and dependable way to collect data that is distributed across CPS and integrate it into actual big data, then artificial intelligence (AI) will be able to manage massive volumes of data, which will result in considerable performance from artificial intelligence. Moreover, if there is a fast and dependable way to collect data that is distributed across CPS and integrate it into actual big data, then there will be an increase in the (AI). Improve Increasing the amount of data that contains massive amounts of information also delivers considerable benefits (such as improved data security), which enables artificial intelligence to outperform humans in additional domains. Increasing the amount of data that contains massive amounts of information also delivers considerable benefits . According to the findings of a recent study, even the most fundamental AI algorithms are already easily accessible. The problem that has to be solved is determining how to accurately and securely transmit data. This is the question that needs to be answered. Fortunately, the blockchain technology provides a viable way to achieve this goal through a network-wide consensus mechanism that assures tamper-proof data exchange with economic incentives . This is made possible by the technology. The term "blockchain" refers to a type of digital ledger that may record transactions and is shared across a network. Therefore, the utilisation of blockchain technology to ensure the confidentiality of the data transfer might result in future advancements in artificial intelligence. This makes it possible for artificial intelligence to draw conclusions that are more reliable on the basis of the huge volumes of data collected from more locations all over the Internet. meet. For example, if many paradigms of edge computing are used in tandem with one another, the overall performance of an edge network may be increased [4]. This can be accomplished by coordinating their use. Blockchain technology makes it feasible to develop dependable processes because of its ability to provide a trustworthy and tamper-proof architecture for metadata [5]. This infrastructure is required in order to significantly re-encode all of the data that is consumed. As a result of this, SecNet has created a data exchange mechanism that is built on blockchain technology and has guaranteed characteristics. Additionally, SecNet provides economic incentives between various units by embedding smart contracts in the data to trigger tamper-proof automated value exchanges when sharing data or exchanging security services. These value exchanges can be triggered when sharing data or exchanging security services .These exchanges of value can take place concurrently with the sharing of data or the trading of security services. To do. In this way, SecNet protects the data you provide and makes it simpler for the CPS to share information with other organisations. In addition, the data , which acts as "fuel" for the AI, might be of considerable value in some situations [6].

Literature Survey

H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, (2018) A decentralised and trustworthy computer and networking model known as the hyper linked network. A sophisticated CPS system has surfaced alongside the growth of the Internet of Things, and it is quickly developing into a potentially fruitful information infrastructure. When it comes to the CPS system, the loss of control over user data has become a very major concern, making it impossible to preserve users' privacy, stimulate innovation, and ensure that data remains in the custody of the appropriate parties. As a solution to the problem of losing control over one's data, we suggest in this article HyperNet, which is an innovative paradigm for decentralised trustworthy computing and networking. The existing communication-based information system has the potential to be transformed into the data-oriented information society of the future thanks to the capabilities of HyperNet, which include the capacity to defend data sovereignty. The Internet of Things (IoT) is a branch of information technology that has seen fast growth thanks to the ongoing development of cloud computing and big data technologies [7].

K. Fan, W. Jiang, H. Li, and Y. Yang, (2019) A lightweight RFID protocol for medical privacy in IoT. RFID supports the Internet of Things. Radio frequency identification technology in healthcare might address patient confidentiality. The reader lets The RFID tags included into the system capture data, which is then analysed by a back-end server. Amber is a type of architecture that has the capacity to partition user data from the applications that make use of it, while at the same time providing programmes with significant global querying capabilities to locate user data. We show how multi-user

applications such as email may potentially employ global queries to gather and monitor data that is important to other users in a more effective manner than is now possible. Amber gives users the ability to select which programmes have access to and share their data. Amber gets rid of the need for application-specific data partitioning, making it possible for a new category of programmes [8].

Zheng Z, Dai H, Wu J.(2019) The phrase "artificial intelligence" refers to a large area that spans a range of subfields, some of which include "machine learning" and "cognitive computing." In these subfields, computers are designed to emulate human cognitive skills including as learning and problem solving. However, the computers are often able to duplicate these abilities in ways that are substantially quicker and more precise. The use of artificial intelligence is expanding into a broad variety of new fields, including voice recognition, facial recognition, medical diagnosis, financial forecasting, disease outbreak tracking, and many more. AI algorithms provide computing systems the ability to think and behave in a manner that is geared toward the successful completion of a certain goal or set of goals. There is a possibility that the adoption of AI technologies will increase user and stakeholder safety. These technologies can take advantage of the blockchain technology to open up new routes for acquiring data and learning from it, all without claiming ownership of the data in issue or having control over it". As a consequence of this, there is a potential decrease in risk for not just the corporation but also the stakeholders that contributed the data. It is in everyone's best interest to include privacy-related AI functionality into the architecture of blockchain networks and procedures as early on in the process as is reasonably practicable. This should be done as soon as it is practical to do so. This is true not just for the individuals that participate in a blockchain, but also for the organisation or group that is tasked with defining the governance rules and processes for the blockchain [9].

Bertino E, Kundu A, Sura(2020) Z We are able to distinguish between four distinct groups of stakeholders that may be impacted by the data transparency and privacy practises of a company. The first category consists of the people who took part in the study, from whom both direct and indirect data were collected[26]. The second group consists of victims, who are those who are negatively impacted by decisions that were made based on participant data. The third category consists of those who use the data collected from participants in their own work. The fourth group is custodians, which are those responsible for the management and protection of data. When artificial intelligence can be used to both regulate access to data and develop analytical models based on that data, everyone who has an interest in the system stands to benefit from its implementation [10].

ElGayyar M, ElYamany H, Grolinger K, Capretz (2021)Blockchain technology makes it possible for organisations to protect the privacy of individuals, which is an essential component of self-sovereign identity. Users of a system or collection of systems generally have something that is known as a federated identity. Individuals can use a federated identity, which is a single identity, to access services or information platforms that are provided by multiple parties. This is accomplished through the use of single sign-on (SSO) authentication, which enables individuals to use a single identity and determines that identity. In the past, users of a system or collection of systems owned this kind of identification. Imagine a network of healthcare providers that includes many different types of facilities, such as hospitals, insurance companies, and urgent care clinics. The service providers that are part of this network make it possible for users to access all of the services using a single set of credentials or a digital identity that is federated. This form of identification, which is often managed and stored in a centralised location by a service provider, is susceptible to security problems as a result of the location in which it is managed and stored as well as the way it is handled [11].

"Data security is a fundamental concern for any network architecture, and it is also the foundation for improving artificial intelligence algorithms, which require vast amounts of data from as many diverse locations on the Internet as is practically possible . Amber is a proof-of-concept architecture that demonstrates the work done by T. Chajed and J. Gjengset (2015) and demonstrates that it is feasible to isolate data from web applications. Amber was designed. [12] This provides users of online services with advanced query skills that can be applied anywhere on the web to obtain personal data. Additionally, it grants users of online services control over their own personal data. In order to extend the applicability of the data and application decoupling mechanism beyond simple web services and to all other types of applications, one of the research groups at the Media Lab at the Massachusetts Institute of Technology is working on developing open PDS . The author of the J.-H. Lee (2018) essay is working on building a system called Origin Chain that will provide metadata transparency and operational security. This will allow for the tracing of things all the way through the supply chain. Origin Chain makes it possible for all linked parties to access the same data, which can be relied upon, and makes it simpler for them to respond to shifting environmental conditions and legal mandates [13]. The authors of the 2017 article produced by Q. Xia and E. B. Sifah have suggested the implementation of a MeDShare system that is based on blockchain technology. This system was developed to efficiently maintain and preserve medical records, in addition to facilitating the transmission of medical data between different cloud repositories. Data transfer, auditing, and control are all included in this aspect. Guaranteed. The study that is provided in provides a complete account of the history of blockchain technology and intrusion detection systems (IDS). It also discusses how blockchain technology may be used to IDS and rationalises any potential hidden risks connected with advancing in this direction [14]. Try to guess what could happen. Additionally, the study that was carried out by J. Wang, M. Li, Y. He, H. Li, and K. (2018) develops a blockchain-based incentive system for the use of cloud sensing application software. Your data and the privacy of your interactions are safeguarded as a result of this. In addition to this, it offers the possibility of gaining a promotion. The study that was presented provided a complete analysis of the application of artificial intelligence (AI) to big data and the application of

big data to AI, as well as some potential future areas for development, such as the enhancement of data security using AI [15] The study was presented in. The research that is presented in highlights the fact that the performance of artificial intelligence (AI) improves when a large quantity of data is supplied in order to create a better fundamental model, and that this data needs to be larger and more useful in order to use AI more effectively. The research is presented in [16] We need additional labour in order to generate a dataset, hence we are looking for it. Create the possibility for data security. In addition to this, the study provides a comprehensive analysis of AI tactics that may be utilised in the field of cybersecurity and discusses these methods. It is imperative that it be made clear that the phrases "HyperNet" and "SecNet" are not synonymous with one another in any way. In addition, the goal of SecNet is to make the internet a safer place by sharing not only user data but also security rules that have been generated by AI, whereas the goal of HyperNet is simply to exchange user data in a secure manner. This can be contrasted with the objective of SecNet, which is to make the internet a safer place by sharing not only user data but also security rules that have been generated by AI. is. Last but not least, the PDC is only one of the data storage techniques that are provided by SecNet (for further information regarding this topic, please refer to Section V), whereas HyperNet only provides one.

SECNET'S ARCHITECTURE

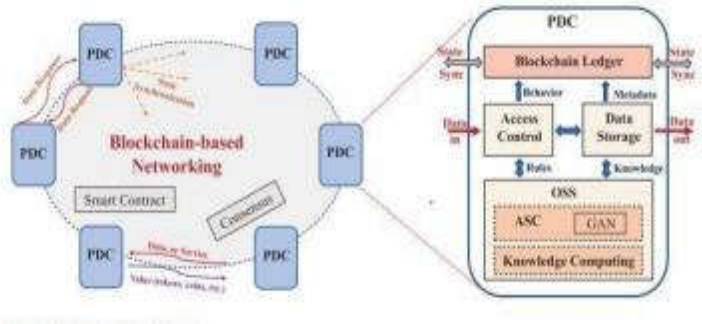

Figure 1: Architecture of secenet

The following three fundamental components are incorporated into SecNet in order to offer a cyberspace infrastructure that is more resistant to cyberattacks: 1) A transaction involving data that is underpinned by blockchain technology and ensures ownership. 2) A secure computing platform that is based on artificial intelligence and makes use of large amounts of data to provide intelligent and dynamic security rules. 3) A reliable alternative to the current method for the purchase of security services the node's state with relation to the other nodes in the network. When it comes to data technology, every node in a SecNet network is equipped with a data storage module as well as an access control module" to guarantee the privacy of any information that is kept on the node [17].

Data Sharing Guaranteed By Block chain

The transfer of data between parties that cannot be trusted is safeguarded by SecNet, which is a blockchain-based data protection system. This safeguarding method provides data protection. The management of the private data centre (PDC) that was originally carried out by HyperNet has been transferred to SecNet. To integrate. A cutting-edge architectural and technological approach is put into place at the PDC in order to facilitate the operation of an AI-based OSS. This is done in addition to the high level of physical protection that is offered to the data. PDC is not complete without the capability of controlling access to data in a standardised manner. The control of access to uniform data is comprised of two distinct parts. It is needed that any data that will be transferred over the internet be registered with the DRB in order for the DRB to alert users of the availability of data transfers. The DRB can do this by sending out notifications to users. The DRB is responsible not only for identifying the data but also for validating the data and documenting the behavior of the interactions that the data have with one another. In addition, the DRB is responsible for naming the data.

AI-based secure computing

The raw data may be updated to generate a number of different sorts of data that can be produced in line with the many different situations and requirements that can develop, and the data are incredibly significant to the owner. For instance, you are able to take user health information that is now kept in a PDC and reorganise it such that it is organised as medical data. This may be done in a number of different ways. Several distinct approaches are possible for achieving this goal. Medical research centres, hospitals, and software designers working on medical application software will find this information to be very helpful. After intensive development and categorization by the GAN module, the OSS of the PDC has become significantly more intelligent and powerful, and fraudulent access requests to data have limited opportunity to compete with this PDC secure and intelligent operating system. Following a significant amount of generation and classification performed by the GAN module . The Text Encompassed in Paraphrase Separate entities now have the capacity to safely communicate their computations with one another in order to improve performance while also lowering their overall energy consumption without compromising the reliability of the blockchain[18].

AI-based secure computing

In addition to the hazards about data security that are inherent in all PDC, the Internet carries with it a distinct set of threats of its own. For instance, a broad variety of "cyberattacks and computer viruses are continuously travelling across the

Internet and are also constantly expanding, both of which result in insufficient protection from the perspective of individual personal data computers (PDCs). After the usage of the smart contract, the access token is issued by the smart contract itself.[40] Because of access tokens, customers are allowed the ability to obtain the required data from the storage system at the correct address. SGX protects the process of value exchange and makes certain that the user does not in any way delay the processing of intelligent contracts. The execution of SGX-based smart contracts allows the blockchain ledger to handle the process of value exchange. This enables the blockchain ledger to handle the process of handling transactions.

USE SCENARIO

SecNet enables a wide variety of applications that make use of artificial intelligence (AI) and embedding that is special to blockchain technology. Implementing and making use of SecNet typically results in one of the most prevalent uses, which is the sharing of medical information between parties that each other trust. This contributes to the provision of an environment that is both intelligent and secure for the handling of medical data. This is the facet of the healthcare system that bears the utmost significance across the board in every country.

Necessaries of Implementing Secnet for Medical Care

The establishment of SECNET is very necessary for the transportation of medical goods. When it comes to the creation of a unified health care system for the entire world, the traditional methods that are used to organise medical data are inefficient. On the one hand, in the modern world, medical records are stored in a wide variety of distinct healthcare facilities and are maintained by a wide variety of distinct organisations, each of which may have distinctive needs from a financial and operational standpoint. The components that make up SecNet include a data release guarantee based on blockchain technology, an artificial intelligence-based behavioural analysis system, and a smart contract that controls interactions between trustworthy organisations. These parts were developed in order to provide solutions to the problems that were discussed before. Make use of in order to achieve the goal of properly identifying the source of secure computing and data. - In addition to activity tracking, provides auditing and regulating capabilities as a component of an open fraud prevention strategy. The following is an exhaustive protocol that was provided by SecNet in order to carry out a reliable transmission of the medical data that is encoded in these characters.

Alternative Way for Secnet

It is the responsibility of the PDC to provide storage for the SecNet data, and it is the responsibility of the owner of the PDC to ensure that the data is kept in a secure environment. The data remains in the control of its owner in this fashion, and the PDC may be utilised to monitor any interactions that take place with the data on a local level. If, on the other hand, users of SecNet choose to keep their data in a secure cloud that is provided by a well-known and significant organisation that can guarantee the data security" rather than keeping it in their own personal data centres (PDCs), then the InterPlanetary file will be able to operate as intended. This information is the PDC of the data owner, and it is shared across the entirety of SecNet. One such strategy involves the establishment of specific secure computer nodes on the SecNet, through which data can flow but through which you can only respond or not answer questions. It is feasible to expose high-dimensional data without sacrificing data security or user privacy in order to promote AI-based computing and the extraction of information for specific users. This would be beneficial for both of these purposes .

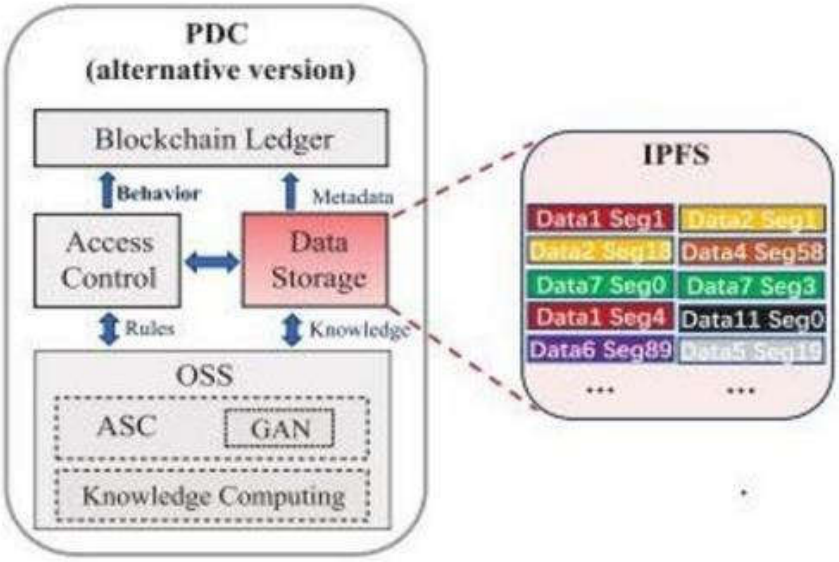

Figure 2: A different storage strategy for secnet

ANALYSIS

One of the forms of network assault that is considered to be among the most serious is known as the distributed denial of service attack. This type of attack is considered to be among the most serious because it has the potential to disrupt both the physical infrastructure of the Internet as well as its 4,444 applications. These kinds of attacks can be used by attackers to cause popular and essential online applications to run out of available bandwidth resources, which will result in customers being unable to access the affected services. This type of attack can also cause customers to be unable to access the affected services. These sorts of attacks can also be employed by attackers to cut off internet connection throughout a significant chunk of the country as a whole. This would imply that SecNet is able to greatly mitigate the effects that well-known DDoS assaults have on their targets. According to the findings, a considerable decrease in the overall number of vulnerabilities that might potentially affect SecNet could be linked to the increased number of standard security regulations that have been put into place. This is as a result of the fact that as the total number of shared security rules rises, everyone who participates in the network gets more educated about the condition in which its security is now found. Because of this, it will be far more difficult for an attacker to effectively carry out and identify a distributed denial of service assault. establishing the benchmark for the criteria that will regulate the safety of broadband connections throughout the bulk of the country. This suggests that SecNet has the ability to significantly reduce the impact that well-known DDoS attacks have. According to the findings, a significant reduction in the total number of vulnerabilities impacting SecNet may be attributed to the number of common security rules that have been implemented.This is due to the fact that as the total number of shared security rules increases, everyone who participates in the network becomes more knowledgeable about the state of its security. As a consequence of this, it becomes more difficult for an attacker to successfully execute and detect a distributed denial of service attack, which raises the bar for the standards governing safety [19].

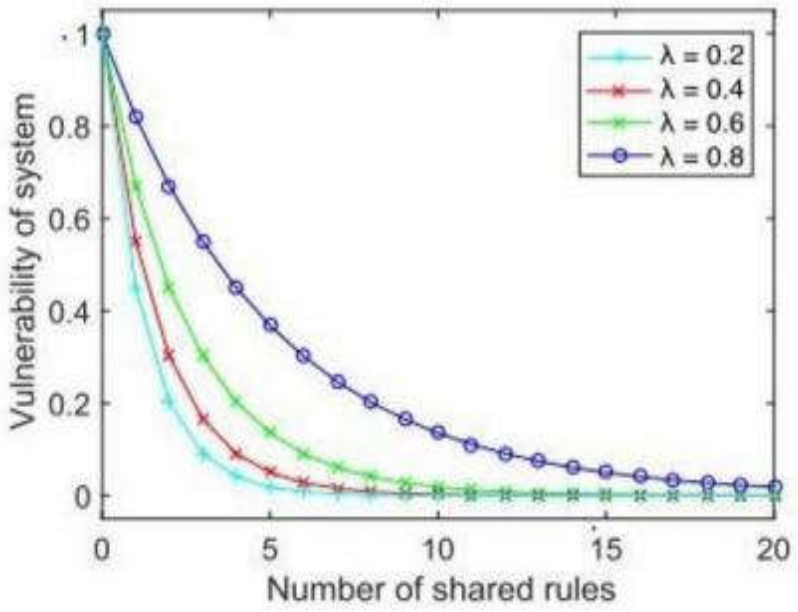

Figure 3: The danger posed by distributed denial-of-service attacks (DDOS) to secnet

When every participant adds their own set of security rules to the blockchain in addition to those contributed by other users, SecNet's overall level of security continues to improve. This is as a result of the fact that each person that participates in the system have substantial security skills to ward against attacks. One of the most crucial elements that plays a role in determining what each member does is the quantity of money that they bring in. Throughout the process of evaluation, there were a total of three distinct pricing points that were studied for general safety rules. These price points were p = 1.05, 1.5, and 2. The ratio of the predetermined price of an item to the item's actual value on the market is the definition of the price level. in the example that was given. The result of the experiment in number 6 shows that there is a good chance that the income of the rule publisher will decrease if the price of the rule that is subject to collusion is set at an unreasonablely high level [20].

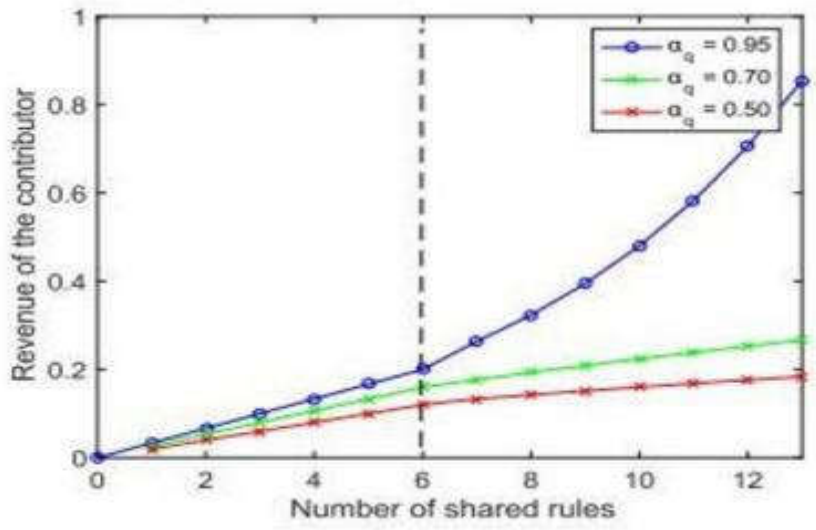

Figure 4: Earnings that emerge from the shared use of varying standards of security rules

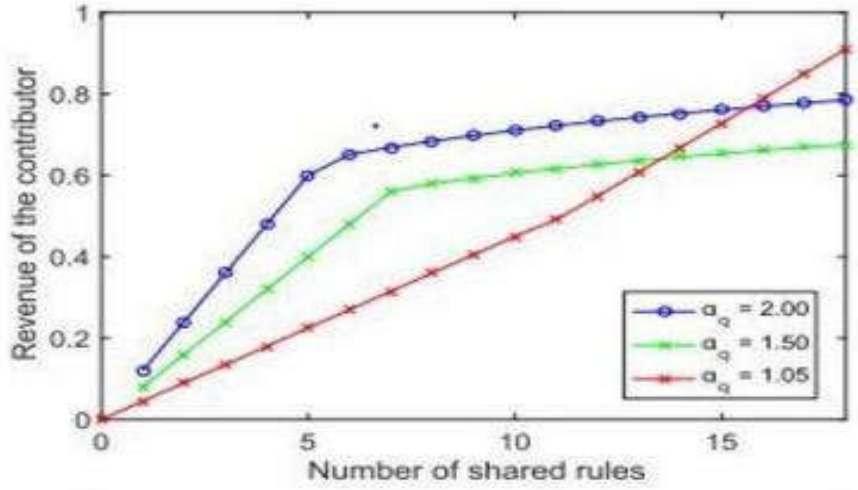

Figure 5: Revenue generated through the distribution of security rules in conjunction with rule pricing

CONCLUSION

SecNet, a novel network architecture focused on safe data, uses AI and blockchain to address data misuse and enable AI to reliably manage data in an unsecured environment. AI and blockchain will address data abuse. Store, share, and compute data instead of trading it . A blockchain-based incentive system, a more powerful AI, and an AI-based secure computing platform will be part of SecNet. SecNet keeps data in the right hands. protects. In addition, it examines a typical usage of SecNet in healthcare systems and offers an alternate storage technique. It concludes with recommendations. It also evaluates network vulnerabilities after DDoS assaults and examines the creative traits that motivate people to contribute security rules to safeguard the network. For network security. Future research will address blockchain technology to authorise data requests, safe and comprehensive smart contracts for data sharing, and AI-powered computing services on SecNet . Research will begin soon. It also mimics SecNet and performs in-depth network performance evaluations on more sophisticated systems.

REFERENCES

[1]. J. Yang, S. He, Y. Xu, L. Chen, J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," Sensors, vol. 19 no. 4,DOI: 10.3390/s19040970, 2019.
[2]. J. Chen, S. Micali, "Algorand: a secure and efficient distributed ledger," Theoretical Computer Science, vol. 777, pp. 155-183, DOI: 10.1016/j.tcs.2019.02.001, 2019.
[3]. L. Demetrio, A. Valenza, G. Costa, G. Lagorio, "Waf-a-mole: evading web application firewalls through adversarial machine learning," Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp. 1745-1752, .
[4]. Dr. Abdul Hannan Abdul Mannan Shaikh, “Blockchain Technology for Beginners”, 1 Nov 2022, Book Nation Press, Ltd. Channai, Tamilnadu, India.
[5]. M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang and S. Sen, (2018) "Enhancing selectivity in big data", IEEE Security Privacy, vol. 16, no. 1, pp. 34-42,.
[6]. A. de Montjoye, E. Shmueli, S. S. Wang and A. S. Pentland,(2014.) "openPDS: Protecting the privacy of metadata through SafeAnswers", PLoS ONE, vol. 9, no. 7,

[7]. H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu and J. Xing,(2018) "Hyperconnected network: A decentralized trusted computing and networking paradigm", IEEE Netw., vol. 32, pp. 112-117.
[8]. K. Fan, W. Jiang, H. Li and Y. Yang, (2018) "Lightweight RFID protocol for medical privacy protection in IoT", IEEE Trans Ind. Informat., vol. 14, no. 4, pp. 1656-1665.
[9]. Zheng Z, Dai H, Wu J.(2019) Blockchain Intelligence: When Blockchain Meets Artificial Intelligence 2020. arXiv preprint arXiv:1912.06485.
[10]. Bertino E, Kundu A, Sura Z.(2020) Data Transparency with Blockchain and AI Ethics. Data and Information Quality; 2019. https://doi.org/10.1145/3312750
[11]. ElGayyar M, ElYamany H, Grolinger K, Capretz M, Mir S.(2021) Blockchain-Based Federated Identity and Auditing. International Journal of Blockchains and Cryptocurrencies. 2020.p. 179-205.
[12]. T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, et al., (2015) "Amber: Decoupling user data from Web applications", Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), pp. 1-6.
[13]. J.-H. Lee(2017)"BIDaaS: Blockchain based ID as a service", IEEE Access, vol. 6, pp. 2274-2278,.
[14]. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", IEEE Access, vol. 5, pp. 14757-14767, 2017.
[15]. J. Wang, M. Li, Y. He, H. Li, K. Xiao and C. Wang, (2018) "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications", IEEE Access, vol. 6, pp. 17545-17556,.
[16]. C. Sun, A. Shrivastava, S. Singh and A. Gupta, (2017)"Revisiting unreasonable effectiveness of data in deep learning era", Proc. IEEE Int. Conf. Comput. Vis. (ICCV), pp. 843-852,.
[17]. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han,(2018) "When intrusion detection meets blockchain technology: A review", IEEE Access, vol. 6, pp. 10179-10188,.
[18]. Conti, M., Sandeep Kumar, E., Lal, C., and Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Commun. Surv. Tutorials 20 (4), 3416–3452. doi:10.1109/comst.2018.2842460.
[19]. Azzaoui, A. E., Singh, S. K., Pan, Y., and Park, J. H. (2020). Block5GIntell: Blockchain for AI-Enabled 5G Networks. IEEE Access 8, 145918–145935. doi:10.1109/ACCESS.2020.3014356
[20]. A. B. Kurtulmus and K. Daniel, (2018), "Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain" in arXiv:1802.10185, [online] Available: https://arxiv.org/abs/1802.10185.