Advanced Production and Industrial Engineering
R.M. Singari and P.K. Kankar (Eds.)

doi:10.3233/ATDE220751

IOT Based Privacy Preserving Machine Learning Algorithm for High-Speed Encryption

Ankit AGGARWAL[a] , Sneha ARORA[b]

[a]*Bachelors of Technology, Department of Chemical Engineering, Manipal Institute of Technology, Karnataka, India*

[b]*PhD Scholar, Department of Electronics and Communication, Lovely Professional University, Punjab, India*

Abstract Many of our ordinary things will soon be linked, due to contemporary Internet of Things (IoT) technology. These items will be able to connect and interact with one other as well as their surroundings, automating much of our job. Security, seamless authentication, resilience, and simplicity of maintenance are essential for IoT node communication. Blockchain appears as a possible option to provide these vital features. Blockchain's decentralised nature has enabled it to address several IoT security, maintenance, and authentication issues. As a consequence, the number of blockchain-based Internet of Things applications has increased dramatically in recent years. This study presents a blockchain-based industrial IOT method using RSA encryption. RSA encryption results in fast encryption.

Keywords- machine learning, encryption, security, IOT

1. Introduction

The Internet of Things (IoT) is comprised of a vast number of devices that generate, process, and transmit massive volumes of security and safety-critical data, as well as personally identifiable information. As a result, they are attractive targets for a wide range of cyber assaults. [1,] Many of the new networkable devices that make up the Internet of Things are low-energy and lightweight, making them particularly well suited for usage in densely populated metropolitan areas like cities. [2] These devices must concentrate the great majority of their available energy and compute resources to the execution of critical application operations as a consequence, making the challenge of providing cost-effective security and privacy protection very difficult [3]. Traditionally used security solutions, both in terms of energy consumption and computer overhead, are sometimes deemed too expensive for the Internet of Things, owing to the high cost of power and the considerable overhead associated with computing. In part because many of today's most advanced security frameworks are very centralised, they are not always well-suited for the Internet of Things, which is hindered by scaling concerns, the one-to-one nature of communication, and the presence of a single point of failure. [4]. Some Internet of Things apps may find it difficult to provide personalised services as a result of the fact that present methods of protecting user privacy often reveal noisy or erroneous information. [5]. When it comes to designing a security and privacy solution

that is lightweight, scalable, and distributed, the emergence of the Internet of Things is essential. Because of its distributed, secure, and private nature, Blockchain (BC) technology has the potential to address the concerns mentioned above. It is the technology that powers Bitcoin, which is widely regarded as the world's first cryptocurrency system [6]. Blockchain technology is a kind of distributed ledger technology. As a consequence of the increasing use of Internet of things (IoT) devices in a variety of applications, the security and privacy of consumers have come to the top of the priority list for policymakers. As a result of poor eating habits and a lack of knowledge about health-conscious foods available on the market, new diseases are being introduced at an alarming rate in the United States, and the severity of existing illnesses is increasing as a result of these factors. More than ever before, the Internet of Things (IoT) is gaining attention because it has the potential to reduce the severity of disease by allowing patients to know the present condition of their ailment via the use of IoT devices that are based on dynamic inputs from the human body. Furthermore, the convergence of Internet of Things (IoT) and cloud computing technologies is playing an increasingly crucial role in the delivery of e-health services, which should be taken into consideration. Due to the fact that security is a basic goal in this environment, data storage and transmission are complicated tasks in this environment [7].

Recent years have seen an alarming surge in cyber threats, and current security and privacy solutions are becoming more ineffective and outdated as a result. For hackers, this means that everyone who is connected to the Internet has the potential to be a source of income [8]. The result is that Machine Learning (ML) approaches are being used to massive intricate datasets in order to provide reliable outputs, and the outputs gained may be used to predict and uncover vulnerabilities in Internet of Things-based systems. [9] Blockchain technologies, in particular, are becoming more popular as a way of resolving security and privacy issues in present Internet of Things applications, and they have the potential to become much more prominent in the future. In the field of machine learning algorithms and Bayesian computing approaches, a significant amount of research has been done [10]. Although these research use machine learning algorithms or behavioural analytics approaches to address security or privacy concerns, they are not sufficiently comprehensive to handle both security and privacy concerns at the same time [11]. It is necessary to conduct a comprehensive evaluation of current attempts to solve both security and privacy problems via the use of machine learning algorithms and behavioural analytics approaches. [12,13] The Industrial internet of things (IIoT) may make choices by updating the methods of collecting data, transferring data, and analysing data that are currently in use. This is accomplished via the use of actuators and sensors, as well as computational interaction capabilities. [14] Machine learning is critical in the context of Industry 4.0, also known as the Industrial Internet, since it allows for the activation of predictive analytics as well as the discovery of significant insights that can be utilised to transform enterprises. [15] Machine learning makes advantage of advancements in computing and interface technologies to enable the analysis of enormous amounts of data, such as those generated by an IIoT-based system, and then leverages the information gained to aid in real-time decision making in complicated situations. Machine learning is gaining in popularity all of the time [16]. In response to the growing popularity and reputation of Internet of Things technology and devices, the number of IoT users and devices continues to grow gradually, and the volume of data flowing between devices and users continues to grow at an alarmingly rapid rate as well, according to the latest statistics. The International Telecommunication Union (ITU) has

said that the concerns of users' privacy are just too important to be ignored in the context of what has been dubbed the Internet of Things (IoT) phenomenon. Because of the widespread use of sensors, the capacity to acquire personal information has been significantly enhanced in recent years. Sensors installed into automobiles, buildings, and common settings that can be traversed by people and animals and that can be connected to one another so that they may interact with one another whether they are on the same site or in a separate location are also required to enable integrated services. It is possible to gather precise and complete information about a given area by employing a number of technologies, such as GPS, cameras, and radio frequency identification (RFID). For example, the device's position and bodily indicators such as (illness), pulse, and blood pressure are all recorded in this information [17]. It is possible to collect accurate and comprehensive information about a specific area since the Internet of Things combines a variety of devices such as GPS, cameras, and radio frequency identification [18].

Because of this, the Internet of Things' potential to capture personal information has expanded in tandem with the Internet's ability to develop, resulting in an increase in the amount of information that can be collected. The Internet of Things has the potential to attract the attention of hackers as a result of a variety of issues, including political and commercial objectives [19]. This is especially true when one considers the widespread use of Internet of Things technology across a wide range of sectors, the military and national defence systems, and a number of other exciting fields, among others. As a consequence of the one-of-a-kind internet virus and the acts of hackers, they will cause significant environmental damage. The two risks stated above, when it comes to the Internet of Things, constitute a serious threat to the security of personal information stored on the device. Unfortunately, academics are not paying enough attention to the issue of protecting personal information, which is a shame. In the opinion of a number of experts [20], the current encryption technologies are capable of resolving the security and privacy concerns that arise in the Internet of Things environment.

Despite the fact that Internet of Things (IoT) devices are often the weakest link in a company's network, they are very beneficial to the operations of the company in which they are installed. [21] As a result of their scalability, it is not difficult to see why firms are continuing to extend their usage of them in their operations. Purchasing more equipment is important for cybersecurity teams in order to keep track of all the devices and maintain network security, according to the National Cybersecurity Alliance. [22]

Using high-level machine learning, according to the researchers, it is possible to contribute to the protection of the Internet of Things by automating the scanning and administration of IoT devices throughout the whole network [23-24]. When they scan all devices linked to a network, they may identify potential threats and shut them down quickly, before IT professionals are even aware of the situation. [25]

2. Implementation

In various techniques researchers have used Authors have stated that in future work they will investigate new ways to enhance or reduce the encryption time of deep learning or machine learning models. As an extension to this work, we are using the RSA algorithm, which is much faster in execution than the AES algorithm, to provide privacy to deep learning or machine learning models. As an addition, we are employing the RSA

technique to solve the issue stated, where the author wishes to lower the execution time delay]. The primary graphical user interface (GUI) is shown in Figure 1.

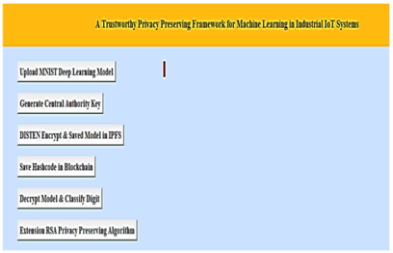

Fig.1 Main GUI

Figure 2 shows the model after it has been loaded, and Figure 3 depicts the encryption using the AES technique. AES was released by the National Institute of Standards and Technology (NIST) in 2001. It was a standard for the encryption of electronic data that had been created by the United States and published by the National Institute of Standards and Technology (NIST). Despite the fact that it is more difficult to install than DES and triple DES, AES is widely used today since it is much stronger than the alternatives. AES is a block cypher, which implies that it encrypts data in chunks rather than in a single piece.

Fig. 2 Loading Dataset Model

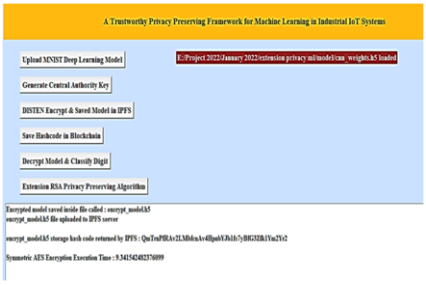

Fig. 3 AES encryption

Figure 4 illustrates the storing of a hashcode in a blockchain. Using traditional storage systems as a starting point On the blockchain, the only thing we save is a hash of our data, which is all that we need. A transaction's cost is kept to a bare minimum since the hash is quite modest in comparison to the amount of data being sent. In terms of how the raw data is stored, we have total control over the process. As an example, it is feasible to make use of a relational database or even just a simple file system. Figure 5 depicts the decoding of character number 4 as shown in the text. Data decryption is the act of converting encrypted data back into its original form, and it is often employed to safeguard sensitive information. In the great majority of instances, the encryption process is being reversed at the time of the incident. Because decryption necessitates the use of a secret key or password, it decodes the encrypted information in such a manner that it can only be decrypted by a user who has been granted access to it.

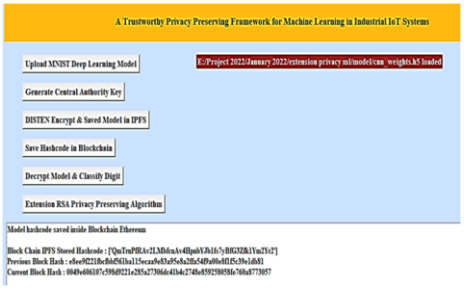

Fig. 4 Hash code in blockchain

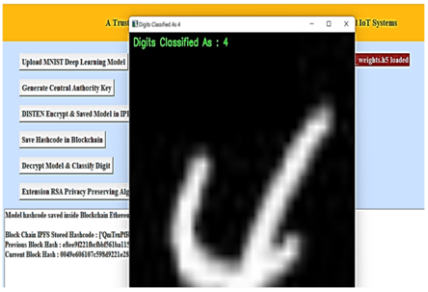

Fig. 5 Decryption

3. Results

As an asymmetric encryption method, RSA encrypts information with the use of both a public key and a private key, rather than just one, as opposed to symmetric encryption techniques (i.e two different, mathematically linked keys). Even though the terms "public key" and "private key" refer to keys that are both shared with the general public, private keys are strictly confidential and must not be shared with anyone else. The RSA algorithm (Rivest-Shamir-Adleman) is the cornerstone of a cryptosystem, which is a collection of cryptographic algorithms that are used to provide certain security services or to accomplish specific security objectives. The RSA algorithm (Rivest-Shamir-Adleman) is used to encrypt data using a public key system. Security software is often used to safeguard sensitive data, particularly data that is shared over insecure networks, from unauthorised access. Because of the use of blockchain, our dataset model approach for encryption and decryption, as shown in the previous image, has a quicker encryption time than the proposed RSA algorithm, as demonstrated in the following figure. It is commonly utilised insecurely by IoT makers in a number of contexts, despite the fact that RSA is considered a secure technology by the industry. It is estimated by the FBI that factoring assaults are responsible for the compromising of more than one in every 172 RSA keys. ECC is a more secure solution when compared to RSA because: ECC keys are smaller and more secure than RSA keys because they do not rely on random number generators; ECC keys are lesser and more secure than RSA keys because they do not rely on random number generators; ECC keys are smaller and more secure than RSA keys since they do not rely on random number generators (RNGs).

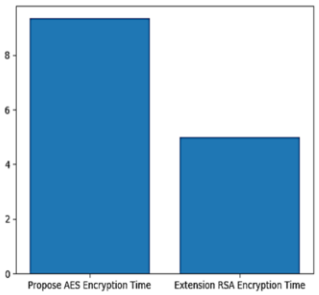

Fig. 6 RSA encryption Output Result

4. Conclusion

The Industrial Internet of Things (IIoT) is ushering in revolutionary change across a broad range of sectors, including energy, agriculture, mining, shipping, healthcare, and everything in between. From energy to agriculture, mining, shipping, and healthcare, and everything in between, the IIoT is ushering in revolutionary change. The Internet of Things (IoT), in addition to making significant use of machine learning (ML) to make use of the huge interconnectedness and large amounts of IIoT data, is a primary driving factor behind the Fourth Industrial Revolution (FIR). Due to the fact that it is a basic driving element of the Fourth Industrial Revolution, the Internet of Things (IoT) is a vital driving force behind the Fourth Industrial Revolution. The blockchain-based Internet of Things network, on the other hand, is open to the public, which implies that, in the event of a security breach, transactional information and encryption keys are made accessible to everyone on the network. It follows as a result that any attacker may get sensitive information about users from this publicly accessible infrastructure without the users even being aware of what is occurring. In order to address this issue, this research delivers output for high-speed encryption with a high degree of security for IOT applications in the industrial context.

References

[1] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe and M. Atiquzzaman.A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6092-6102, Sept. 2020, doi: 10.1109/TII.2020.2974555

[2] Chamikara, M.A.P. & Bertok, Peter & Khalil, Ibrahim & Liu, Dongxi & Camtepe, Seyit & Atiquzzaman, Mohammed. (2020). A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Transactions on Industrial Informatics. PP. 1-1. 10.1109/TII.2020.2974555.

[3] Hussain, Fatima & Hussain, Rasheed & Hassan, Syed & Hossain, Ekram. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2020.2986444.

[4] Parikshit N. Mahalle; Poonam N. Railkar.Identity Management for Internet of Things. Identity Management for Internet of Things , River Publishers, 2015, pp.i-xx.

[5] F. Restuccia, S. D'Oro and T. Melodia.Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4829-4842, Dec. 2018, doi: 10.1109/JIOT.2018.2846040.

[6] Niu, Ben & Zhang, Likun & Chen, Yahong & Li, Ang & Du, Wei & Cao, Jin & Li, Fenghua. (2020). A Framework to Preserve User Privacy for Machine Learning as a Service. 1-6. 10.1109/GLOBECOM42002.2020.9322322.

[7] Bagaa, Miloud & Taleb, Tarik & Bernal Bernabe, Jorge & Skarmeta, Antonio. (2020). A Machine Learning Security Framework for IoT Systems. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2996214.

[8] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki.Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019, doi: 10.1109/COMST.2019.2896380.

[9] Chaabouni, Nadia & Mosbah, Mohamed & Zemmari, Akka & Sauvignac, Cyrille & Faruki, Parvez. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2019.2896380.

[10]F. Hussain, R. Hussain, S. A. Hassan and E. Hossain,.Machine Learning in IoT Security: Current Solutions and Future Challenges,.IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi 10.1109/COMST.2020.2986444.

[11] O. Salman, I. Elhajj, A. Chehab and A. Kayssi.Software Defined IoT security framework.2017 Fourth International Conference on Software Defined Systems (SDS), 2017, pp. 75-80, doi: 10.1109/SDS.2017.7939144.

[12] Li, Shancang & Tryfonas, Theo & Li, Honglei. (2016). The Internet of Things: a security point of view. Internet Research. 26. 337-359. 10.1108/IntR-07-2014-0173.

[13] Khattab, Ahmed & Youssry, Nouran. (2020). Machine Learning for IoT Systems. 10.1007/978-3-030-37468-6_6.

[14] J. Cañedo and A. Skjellum.Using machine learning to secure IoT systems.2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016, pp. 219-222, doi: 10.1109/PST.2016.7906930.
[15] M. Al-Rubaie and J. M. Change.Privacy-Preserving Machine Learning: Threats and Solutions. IEEE Security & Privacy, vol. 17, no. 2, pp. 49-58, March-April 2019, doi: 10.1109/MSEC.2018.2888775.
[16] R. Shokri and V. Shmatikov. Privacy-preserving deep learning. 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2015, pp. 909-910, doi: 10.1109/ALLERTON.2015.7447103.
[17] H. C. Tanuwidjaja, R. Choi, S. Baek and K. Kim. Privacy-Preserving Deep Learning on Machine Learning as a Service—a Comprehensive Survey. IEEE Access, vol. 8, pp. 167425-167447, 2020, doi: 10.1109/ACCESS.2020.3023084.
[18] M. Zolanvari, M. A. Teixeira and R. Jain. Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning. 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), 2018, pp. 112-117, doi: 10.1109/ISI.2018.8587389.
[19] Mohanta, Bhabendu & Jena, Debasish. (2021). Internet of Things Security Using Machine Learning. 10.1007/978-981-15-5243-4_11.
[20] Ahmad, Rasheed & Alsmadi, Izzat. (2021). Machine Learning Approaches to IoT Security: A Systematic Literature Review. Internet of Things. 14. 100365. 10.1016/j.iot.2021.100365.
[21] K, Anuradha & Nirmala Sugirtha Rajini, Selvaraj. (2019). Analysis of Machine Learning Algorithm in IOT Security Issues and Challenges. Journal of Advanced Research in Dynamical and Control Systems. 11. 1030-1034. 10.5373/JARDCS/V11/20192668.
[22] A. Qureshi, M. A. Qureshi, H. A. Haider and R. Khawaja.A review on machine learning techniques for secure IoT networks. 2020 IEEE 23rd International Multitopic Conference (INMIC), 2020, pp. 1-6, doi: 10.1109/INMIC50486.2020.9318092.
[23] S. Malik and R. Chauhan. Securing the Internet of Things using Machine Learning: A Review. 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW), 2020, pp. 1-4, doi: 10.1109/ICCDW45521.2020.9318666.
[24] S. Gupta, S. Vyas and K. P. Sharma. A Survey on Security for IoT via Machine Learning. 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020, pp. 1-5, doi: 10.1109/ICCSEA49143.2020.9132898.
[25] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security. IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41-49, Sept. 2018, doi: 10.1109/MSP.2018.2825478.