Development of ADDA (Additional Data) Algorithm for IoT Security and Privacy

Oliver M. Junio(✉) and Jasmin De Castro-Niguidula

Technological Institute of the Philippines, Manila, Philippines
oliverjunio@uphsl.edu.ph, jasniguidula@yahoo.com

Abstract. Internet becomes one of the basic necessity of a person. From simple sharing of data and information, internet nowadays offers millions of things such as free storage, free communication. Privacy and Security Issues are being compromise with the so many things that Internet provided. Billions of IoT devices will be released in the market by 2020 [1]. To secure connection between devices, the researcher added additional security using ADDA Algorithm. This algorithm will add additional blocks to the traditional encryption for additional security to the gateway of a particular IoT device. There are three (3) parameters to be used in this study to provide security and privacy for the IoT sites and devices. These are the accuracy, encryption speed and decryption speed of data. In this study, the researcher explains the step-by-step details how the ADDA algorithm works and make IoT devices secured for day to day use by making a new algorithm. With the results generated, ADDA algorithm gives additional protection to already encrypted data by adding characters based on the algorithm created. The result of encrypting data using ADDA algorithm was exceptional due to high percentage rate of the test conducted.

Keywords: Internet of Things · IoT · Privacy · Security

1 Introduction

Internet offers one thousand and one data and information, publish anywhere and can be access everywhere. The rise of the internet increases cybercrime this include security and privacy issues. There are three (3) identified main factor that arises the growth of internet this includes First, the development of small scale technology, Second, the inexpensiveness of the technology, and third the presence of online storage [1].

In 2020, 24 Billion of IoT Devices will be released in the market. Along with the development of the technology, is also the growth of security issues such as (1) Public Perception, (2) Vulnerability to Hacking, (3) Readiness of Company to handle security issues and (4) which of the security provider really provides security. Another concern is the privacy issues accompanied to IoT such as (1) uncontrollable volume of data, (2) Unwanted Public Profile, (3) arise of eavesdropping and (4) consumer confidence of finding everything via Internet [2].

IoT revolutionizes how individuals and corporations interact with one another. Security and privacy issues can be resolved by means of competitive advantages network technologies has been developed over the years. Direct connections to a server

J. J. Jung et al. (Eds.): BDTA 2017, LNICST 248, pp. 9–18, 2018.
https://doi.org/10.1007/978-3-319-98752-1_2

can be limited or track down by means of embedded electronics, a good software engineer and administrator plus a good connectivity [3].

Based on the survey done by the internet world stats usage and population statistics, Philippines ranked 15 out of 20 to the top 20 countries with the highest number of internet users having 102,624,209 population and 54,000,000 registered internet users. This means that Internet is part of Philippine community daily living. The inexpensiveness of the technology cost i.e. the production of mobile or smart phone that offers internet connections and the low cost of communication provider are some of the factors that causes the growth of internet usage [4].

With the growing number of Internet users and providers together with the information published via world wide web this paper aims to determine IoT security and privacy issues in the Philippines.

This paper is organized as follows: Sect. 1 defines the state of the internet and IoT security and privacy. Section 2 introduces related work. Issues on privacy and security is discussed in Sect. 3, Sect. 4 shows the different mechanism on how issues on privacy and security can be prevented and Sect. 5 provides conclusions. There are three (3) parameters to be used in this study to provide security and privacy for the IoT sites and device. These are the accuracy, encryption speed and decryption speed of data.

2 Related Works

The modernization of communications that offers automatic connection to internet whenever there is an access made it possible for every person. IoT offers (1) SNS (Social Networking Sites), the connection it offers from one point to another point, made a convenience way of sharing files, (2) Cloud storage, where users can access files as long as there are internet connections, (3) Search engine that can dig every simple and complex data needed by the subscribers [5].

Different means of sharing files and how IoT can be a good help to a daily endeavor a person has. Security and privacy of IoT varies from (1) how people use IoT, (2) where it is connected, (3) policy it handles, (4) security algorithms it have and (5) requirements needed to be verified before connection took place. IoT was used as a Librarian main communication with the aid of mobile technology. A sustainable connection to the internet gives the company a minimal expenses of sharing files [6].

When it comes to IoT security, The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy need to be established. An adequate legal framework must take the underlying technology into account and would best be established by an international legislator, which is supplemented by the private sector according to specific needs and thereby becomes easily adjustable. The contents of the respective legislation must encompass the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT [11].

Another research study about privacy challenges from the Internet of Things, these services can be provisioned using centralized architectures, where central entities acquire, process, and provide information. Alternatively, distributed architectures, where entities at the edge of the network exchange information and collaborate with each other in a dynamic way, can also be used. In order to understand the applicability and viability of this distributed approach, it is necessary to know its advantages and disadvantages – not only in terms of features but also in terms of security and privacy challenges. The purpose of this paper is to show that the distributed approach has various challenges that need to be solved, but also various interesting properties and strengths [12].

While the general definition of the Internet of Things (IoT) is almost mature, roughly defining it as an information network connecting virtual and physical objects, there is a consistent lack of consensus around technical and regulatory solutions. There is no doubt, though, that the new paradigm will bring forward a completely new host of issues because of its deep impact on all aspects of human life. In this work, the authors outline the current technological and technical trends and their impacts on the security, privacy, and governance. The work is split into short- and long-term analysis where the former is focused on already or soon available technology, while the latter is based on vision concepts. Also, an overview of the vision of the European Commission on this topic will be provided [13].

Describe developments towards the Internet of Things (IoT) and discuss architecture visions for the IoT. Our emphasis is to analyze the known and new threats for the security, privacy and trust (SPT) at different levels of architecture. Our strong view is that the IoT will be an important part of the global huge ICT infrastructure ("future Internet") humanity will be strongly relying on in the future with relatively few data centers connected to trillions of sensors and other "things" over gateways, various access networks and a global network connecting them. While the infrastructure is globally connected, it is divided into millions of management domains, such as homes, smart cities, power grids, access points and networks, data centers, etc. It will evolve both bottom-up and top-down. An important question is what consequences a bottom-up and top-down construction of the IoT infrastructure has for the security, privacy and trust and what kind of regulation is appropriate [14].

Embedded, mobile, and cyberphysical systems are ubiquitous and used in many applications, from industrial control systems, modern vehicles, to critical infrastructure. Current trends and initiatives, such as "Industrie 4.0" and Internet of Things (IoT), promise innovative business models and novel user experiences through strong connectivity and effective use of next generation of embedded devices. These systems generate, process, and exchange vast amounts of security-critical and privacy-sensitive data, which makes them attractive targets of attacks. Cyberattacks on IoT systems are very critical since they may cause physical damage and even threaten human lives. The complexity of these systems and the potential impact of cyberattacks bring upon new threats [15].

The Internet of Things consists of various platforms and devices with different capabilities, and each system will need security solutions depending on its characteristics. There is a demand for security solutions that are able to support multi-profile platforms and provide equivalent security levels for various device interactions. In addition, user privacy will become more important in the IoT environment because a lot of personal information will be delivered and shared among connected things. Therefore, we need mechanisms to protect personal data and monitor their flow from things to the cloud. In this talk, we describe threats and concerns for security and privacy arising from IoT services, and introduce approaches to solve these security and privacy issues in the industrial field [16].

IoT introduces the usage of technology to both businesses and consumers. The adaptation of technology as part of people daily lives becomes part of the commodity needed by the society. The solutions it offers and the security mechanism injected on it are sometimes neglected by the consumers, for them as long as technology made their lives easier is more than enough [8]

To ensure IoT Security, Fuzzy logic is best to determine the protocols and algorithms included in the selected research sites with respect to its reliability and efficiency in providing security and privacy [9].

One of the research studies shows how IoT Security was implemented in the network layers and how the algorithm was used to provide efficient security mechanism. Protocols such as RSA and EAS are the major protocols used within their selected sites along with the encryption and decryption algorithm fused together with the protocol [17].

With the aid of IoT, Burt (2016) contrast Hahn (2017) on his believes in IoT. In his report to the United States National Security, Burt pointed out that IoT is a big disguise that uses technology as front end and served as a spy back door. This manner of hiding the true identity of provider and subscribers to the public comprises the security and often result to identity theft and eavesdropping problem. Monteiro (2015) uses Fuzzy logic to provide results for reliability and efficiency in checking the security and privacy to IoT device data which is the same in this study with the help of ADDA algorithm.

3 Methodology

Rapid Application Development was used in creating ADDA algorithm using Visual Studio 6.0.

The researcher used experimental approach to obtain the result of accuracy, encryption speed and decryption speed of data inputted into the IoT device.

To secure connection between devices, the researcher added additional security using ADDA Algorithm. This algorithm will add additional blocks to the traditional encryption for additional security to the gateway of a particular IoT device.

Figure 1 shows how the proposed method constitutes of encrypted data. The ADDA Algorithm will get the encrypted data and will add additional block and pattern that will add confusion and diffusion to possible attack.

Encryption Algorithm

```
Step 1: Get the encrypted data.
Step 2: For every 4 bits of block add additional block.
Step 3: Add New character to the additional block.
```

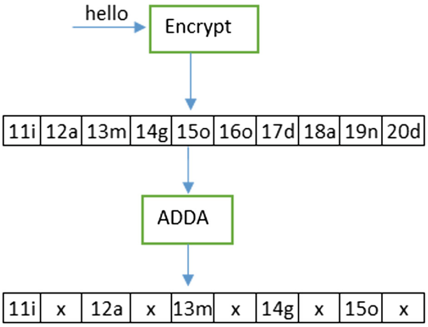

hello
Encrypt
11i 12a 13m 14g 15o 16o 17d 18a 19n 20d
ADDA
11i x 12a x 13m x 14g x 15o x

Fig. 1. ADDA algorithm

Step 4: Place each data to each equivalent container.
Step 5. Save the new encrypted data.

Figure 2 shows the ADDA algorithm program. It composes of command buttons (open file, copy to source folder, 1st Encryption, 2nd encryption (ADDA), decryption and exit system.

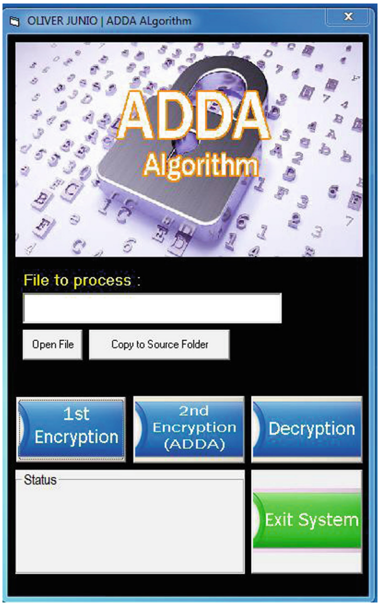


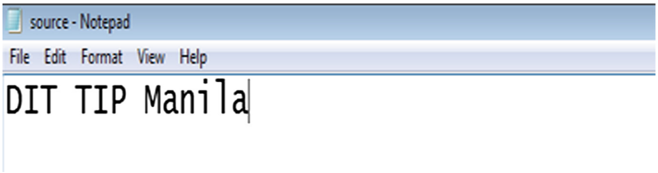
Fig. 2. Adda algorithm main program

4 Results and Discussion

To visualized and see how ADDA algorithm works, following figures were presented.

Encrypting Text

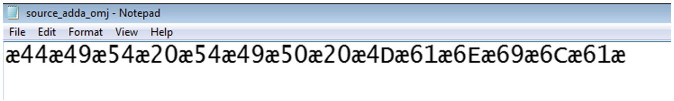
Figure 3 shows original text file named source.txt which will be encrypted later.



```
DIT TIP Manila
```

Fig. 3. Source.txt file

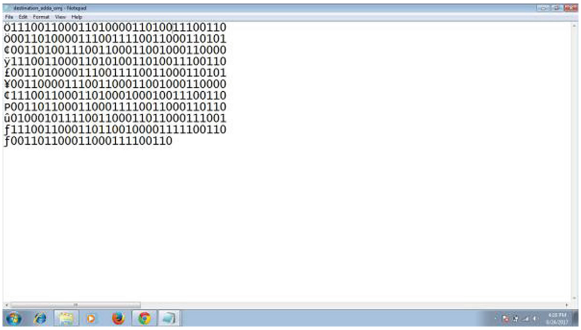
Figure 4 shows the encrypted data (1st encryption command button). The 1st encryption will encrypt the source.txt file by converting characters including spaces into hexadecimal code and in between there is a special character inserted. The source. txt file will be replaced by source_adda_omj.txt.



```
æ44æ49æ54æ20æ54æ49æ50æ20æ4Dæ61æ6Eæ69æ6Cæ61æ
```

Fig. 4. Encrypted text (1st encryption) source_adda_omj.txt file

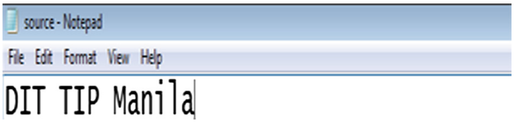
Figure 5 shows the encrypted data (2nd encryption ADDA command button) 0 using ADDA algorithm which every character in Fig. 2 was converted to binary plus in every 4 blocks a randomized special character was being inserted.



```
ö011100110001101000011010011100110
ö000110100001110011110011000110101
¢00110100111001100011001000110000
ÿ11100110001101010011010011100110
£00110100001110011110011000110101
¥00110000111001100011001000110000
¢11100110001101000100010011100110
P00110110001100011110011000110110
û01000101111001100011011000111001
ƒ11100110001101100100001111100110
ƒ001101100011000111100110
```

Fig. 5. Destination_adda_omj.txt file

Figure 6 shows the decrypted data (decryption command button) which brings back the original text and filename (source.txt)



DIT TIP Manila

Fig. 6. The original text and file name source.txt

Figure 7 shows the encryption speed and decryption speed in milliseconds results of data that was encrypted and decrypted. Hardware specification where the program was run is intel core i7 with 8gb RAM running in windows 7 64 bit operating system. It also shows that the decryption speed in most tests conducted was doubled as compared to the encryption speed.

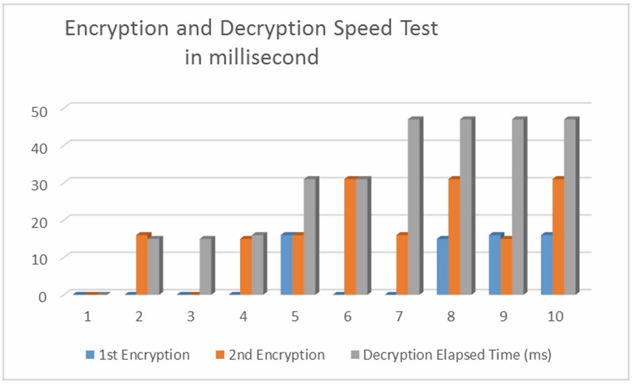


Fig. 7. Speed test report (text file)

Encrypting Image

Figure 8 is the original image that will be encrypted later using ADDA algorithm.

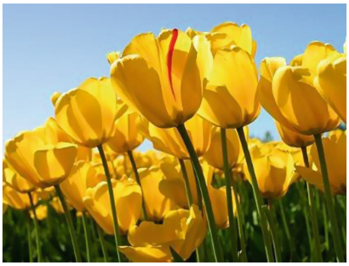
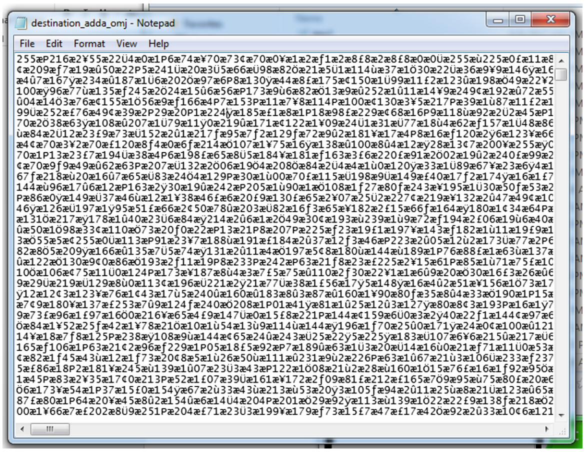


Fig. 8. Original image to be process

Figure 9 is the 1st encryption of the file source.jpg. it took 115752 ms to complete the encryption

Fig. 9. 1st encryption (source_adda_omj.jpg)



```
255æP216æ2¥55æ22Ü4æ0æ1P6æ74æ¥70æ73¢æ70æ0¥æ1æ2æƒ1æ2æ8£8æ2æ8£8æ0æ0Üæ255æù225æ0£æ11æ8
¢æ209æƒ7æ19æû50æ22P5æ241Üæ20æ3Ü5æ66æÜ98æ82Öæ21æ5Ü1æ114ùæ37æ1Ö30æ22Üæ36æ9¥9æ146ÿæ16
æ4û7æ167ÿæ234æû187æ1Ü6æ202Öæ97æ6P8æ130ÿæ44æ8£æ175æ¢150æ1Ü99æ11£2æ123ûæ198æÖ49æ22¥2
100æÿ96æ77ùæ135æƒ245æ2Ö24æ15û6æ56æP173æ9ù6æ82æÖ13æ9æû252æ1û11æ14¥9æ249¢æ192æû72æ55
û04æ14Ö3æ76æ¢155æ1Ö56æ9æƒ166æ4P7æ153Pæ11æ7¥8æ114Pæ100æ¢130æ3¥5æ217Pæ39æ1ù87æ11£2æ1
99Üæ252æ£76æ49¢æ39æ2P29æ20P1æ224ÿæ185æ£1æ8æ1P18æ98£æ229æ¢68æ16P9æ118ùæ92æ2Ü2æ45æP1
70æ2Ö38æ63ÿæ108æû207æ1Ü79æ11ÿ0æ219ûæ171æ¢122æ1¥09æ24Ü1æ31æÜ77æ18ù4æ62æƒ157æ1Ü48æ8€
ùæ84æ2Ü12æ23£9æ73æÜ152æ2û1æ217ƒæ95æ7ƒ2æ129ƒæ72æ9û2æ181¥æ17æ4P8æ16æƒ120æ2ÿ6æ123¥æ6€
æ4¢æ70æ3¥2æ70æ£120æ8ƒ4æ0æ6ƒæ214æÖ107æ1¥75æ16ÿæ138æû100æ8û4æ12æÿ28æ13¢7æ200¥æ255æÿC
70æ1P13æ23£7æ194Üæ38æ4P6æ198£æ65æ8Ü5æ184¥æ181æƒ163æ3£6æ220£æ91æ2Ö02æ19û2æ240£æ99æ2
¢æ70æ9ƒ9æ49æû62æ63Pæ207æÜ132æ2Ö06æ19Ö4æ208Öæ84æ2Ü4æ4æ1ù0æ120ÿæ33æ1Ü89æ67¥æ23æ6ÿ4æ1
67ƒæ218æù20æ16û7æ65æÜ83æ24Ö4æ129Pæ30æ1ù00æ70£æ115æÜ198æ9Üæ149æ£40æ17ƒ2æ174ÿæ16æ1£7
144æù96æ17û6æ12æP163æ2ÿ30æ19ûæ242æP205æ1ù90æ1æÖ108æ1ƒ27æ80ƒæ243æ¥195æ1Ü30æ50ƒæ53æ2
Pæ86æ0ÿæ149æÜ37æ46ùæ12æ1¥38æ46£æ6æ20£9æ130£æ65æ2¥07æ25Ü2æ227¢æ219æ¥132æ2û47æ49¢æ1C
46ÿæ126æÜ197æ1ÿ95æ51£æ66æ2¢50æ78ûæ203æÜ82æ16ƒ3æ65æ¥182æ2£15æ66ƒæ164æÿ180æ1¢34æ64Pæ
æ131Öæ217æÿ178æ1û40æ23Ü6æ84æÿ214æ2û6æ1æ2Ö49æ30¢æ193æù239æ1ù9æ72æƒ194æ2£06æ19ù6æ40æ
ûæ50æ1Ö98æ33¢æ110æÖ73æ20ƒ0æ22æP13æ21P8æ207Pæ225æƒ23æ19£1æ197¥æ143æƒ182æ1ù11æ19£9æ1
3æÖ55æ5æ¢255æ0Üæ113æP91æ23¥7æ188ùæ191æ£184æ2û37æ12ƒ3æ46æP223æ2û05æ12ù2æ173Üæ77æ2P€
82æ8Ö5æ209ÿæ166æû135æ7Ü5æ74æÿ131æ2û11æ4æÖ197æ5¢8æ180ùæ144æù189æ1P76æ88£æ1æ63ùæ137æ
ûæ122æÖ130æ9¢0æ86æÖ193æ2ƒ11æ19P8æ233Pæ242æP63æ21ƒ8æ23æ£225æ2¥15æ61Pæ85æ1ù71æ75£æ1C
10Öæ106æ¢75æ11Ü0æ124Pæ173æ¥187æ8ù4æ3æ7£5æ75æû110æ2ƒ30æ22¥1æ1æ6û9æ20æÖ30æ16£3æ26æû€
9æ29Üæ219æÜ129æ8ù0æ113¢æ196æÜ221æ2ÿ21æ77Üæ38æ1£56æ17ÿ5æ148ÿæ16æ4û2æ51æ¥156æ1Ö73æ17
ÿ12æ12¢3æ123¥æ76æ1¢43æ17ù5æ240ûæ160æû183æ8û3æ87æû160æ1¥90æ80ƒæ35æ8û4æ33æÖ190æ1P15æ
æ7¢9æ180¥æ137æ£253æ7û9æ124ƒæ240æÖ208æ1P01æ41ÿæ81æ1û25æ12û3æ127ÿæ80æ8¢3æ193Pæ16æ1ÿ7
9æ73£æ96æ1£97æ16Ö0æ216¥æ65æ4£9æ147Üæ0æ15£8æ221Pæ144æ¢159æ6Ü0æ3æ2ÿ40æ22ƒ1æ144¢æ97æ€
Öæ84æ1¥52æ25ƒæ42æ1¥78æ21Öæ10æ1ù54æ13ù9æ114ùæ144æÿ196æ1ƒ70æ25û0æ171ÿæ24æ0¢æ100æû121
14¥æ18æ7ƒ8æ125Pæ238æÿ108æ9ùæ144æ¢65æ24ûæ243æÜ25æ22ÿ5æ225ÿæ183æÜ107æ6¥6æ215ûæ217æÜ€
165æƒ106æ1P63æ21¢2æ96æƒ229æ1P05æ18£5æ92æP7æ189ûæ63æ1Ü3æ20æÜ14æ16ù0æ21æƒ71æ11Ü0æ53æ
¢æ82æ1ƒ45æ43ùæ12æ1ƒ73æ20¢8æ5æ1ù26æ50ùæ111æû231æ9ù2æ226Pæ63æ1û67æ21ù3æ106Üæ233æƒ237
5æ£86æ18P2æ181¥æ245æù139æ1û07æ23Ü3æ43æP122æ1Ö08æ21ù2æ28æù160æ1Ö15æ76£æ16æ1ƒ92æ95Öæ
1æ45Pæ83æ2¥35æ17¢0æ213Pæ52æ1£07æ39Üæ161æ¥172æ2ƒ09æ81£æ212æ£165æ7Ö9æ95æù75æ80£æ20æ€
Ö6æ173¥æ54æ1P37æ15£0æ154ÿæ67æ2ù33æ43ùæ213æù53æ20ÿ3æ105ƒæ94æ2û11æ25ùæ8æ21Üæ123æû65æ
87£æ80æ1P64æ20¥æ45æ8û2æ154ûæ6æ14Ü4æ204Pæ201æÖ29æ92ÿæ113æù139æ1Ö22æ22£9æ138ƒæ218æÖ2
00æ1¥66æ7æ£202æ8Ü9æ251Pæ204æ£71æ23Ü3æ199¥æ179æƒ73æ15£7æ47æ£17æ42Öæ92æ2û33æ10¢6æ121
```

Fig. 10. 2nd encryption (destination_adda_omj.jpg)

Figure 11 shows the decrypted image which is exactly the same of the original image.

Table 1 shows the accuracy of image resolution before and after encryption and decryption occurs. The accuracy of the system to bring back the original file in its original resolution is 100%.

Figure 10 shows the encrypted file using ADDA algorithm

Fig. 11. The original image after decryption

Table 1. Accuracy test of image resolution

	Original File Size	Original resolution in pixel	File Size after decryption	Resolution after decryption	Accuracy of resolution after
1	84.4	512 × 384	475	512 × 384	100%
2	84.4	512 × 384	475	512 × 384	100%
3	84.4	512 × 384	475	512 × 384	100%
4	84.4	512 × 384	475	512 × 384	100%
5	84.4	512 × 384	475	512 × 384	100%
6	84.4	512 × 384	475	512 × 384	100%
7	84.4	512 × 384	475	512 × 384	100%
8	84.4	512 × 384	475	512 × 384	100%
9	84.4	512 × 384	475	512 × 384	100%
10	84.4	512 × 384	475	512 × 384	100%

5 Conclusion

Security and privacy are one the major concern of IoT users, with the aid of ADDA algorithm additional security will be added to the traditional encryption. Privacy were protected using two procedures (1) by adding blocks to the original blocks and (2) by randomly inserting special characters. Based on the result, the encrypted data will be more secured and can be used privately since blocks of data are encrypted with the help of ADDA algorithm. The accuracy result of encrypting data using ADDA algorithm was exceptional due to high percentage rate of the test conducted.

References

Smith, M.: Protecting privacy in an IOT – connected world. Inf. Manag. **49**, 36–39 (2015)

Meola, A.: How the Internet of Things will affect security and privacy (2016). http://www.businessinsider.com/internet-of-things-security-privacy-2016-8

Navetta et al.: The Security, Privacy, and Legal Implications of the Internet of Things (IoT) Part One – The Context and use of IoT (2015). http://www.dataprotectionreport.com/2015/05/the-security-privacy-legal-implications-of-the-internet-of-things-iot-part-one-the-context-and-use-of-iot/

de Argaez, E.: Miniwatts Marketing Group, International Division of Miniwatts de Colombia Ltda, Carrera 7, Bogota, Colombia (2017)

Bian, J., et al.: Mining Twitter to assess the public perception on the Internet of Things. PLoS ONE **11**, 1–14 (2016)

Hahn, J.: The Internet of Things: mobile technology and location services in the libraries. Libr. Technol. Rep. **53**(1), 1–28 (2017)

Burt, J.: IoT Could be used by Spies, U.S. Intelligence Chief Says. eWeek, p. 1, 2 December 2016

Patra et al.: Securing IoT devices and gateways (2016). http://www.ibm.com/developerworks/library/iot-trs-secure-iot-solutions1/index.html

Monteiro, E., et al.: Security for the Internet of Things: a survey of existing protocol and open research issues. IEEE Commun. Surv. Tutor. **17**(3), 1294–1312 (2015)

Suo, H.: Security in the Internet of Things: A Review. Guangdong Jidian Polytechnic Guangzhou, China (2012). https://www.researchgate.net/publication/254029342_Security_in_the_Internet_of_Things_A_Review

Weber, R.H.: Internet of Things-new security and privacy challenges. Comput. Law Secur. Rev. **26**(1), 23–30 (2010)

Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed Internet of Things. Comput. Netw. **57**(10), 2266–2279 (2013)

Medaglia, C.M., Serbanati, A.: An overview of privacy and security issues in the Internet of Things. In: Giusto, D., Iera, A., Morabito, G., Atzori, L. (eds.) The Internet of Things, pp. 389–395. Springer, New York (2010). https://doi.org/10.1007/978-1-4419-1674-7_38

Kozlov, D., Veijalainen, J., Ali, Y.: Security and privacy threats in IoT architectures. In: Proceedings of the 7th International Conference on Body Area Networks, pp. 256–262. ICST (Institute for Computer Sciences, Social- Informatics and Telecommunications Engineering), February 2012

Sadeghi, A.R., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial Internet of Things. In: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 1–6. IEEE, June 2015

Hwang, Y.H.: IoT security & privacy: threats and challenges. In: Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security, p. 1. ACM, April 2015

Liu, Y., Zhou, G.: Key technologies and applications of Internet of Things. In: 2012 Fifth International Conference on Intelligent Computation Technology and Automation (ICICTA), pp. 197–200. IEEE, January 2012