FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 270-275 | e-ISSN: 2347-470X

A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT

Addanki Kavitha[1], B Srinivasa Rao[2], Dr Nikhat Akhtar[3], Dr Shaik Mohammad Rafi[4], Prabhdeep Singh[5], Dr Sunanda Das[6] and Dr G Manikandan[7]

[1]Assistant Professor, Department of Computer Science Engineering, P B Siddhartha College of Arts and Science, Vijayawada, Andhra Pradesh, dkavithamuller@gmail.com
[2]Professor, Department of Computer Science Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad-500090, Email: bsrgriet2015@gmail.com
[3]Associate Professor, Department of Computer Science & Engineering, Ambalika Institute of Management and Technology (AIMT), Lucknow, UP, India, dr.nikhatakhtar@gmail.com
[4]Professor, Artificial intelligence and information technology, Sri Mittapalli engineering College, mdrafi.527@gmail.com
[5]Assistant Professor, Department of Computer Science & Engineering, Graphic Era Deemed to be University,Dehradun, Uttarakhand-248002 Email: prabhdeepsingh.cse@geu.ac.in
[6]Associate Professor, Jain University, Kanakpura Road, Bangalore-562112, das.sunanda2012@gmail.com
[7]Assistant Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai-602105, mrg.manikandan@gmail.com

***Correspondence:** Dr G Manikandan; Email: mrg.manikandan@gmail.com

ABSTRACT- The rise of digital technology has essentially enhanced the overall communication and data management system, facilitating essential medical care services. Considering this aspect, the healthcare system successfully managed patient requirements through online services and facilitated patient experience. However, the lack of adequate data security and increased digital activities during Covid-19 made the healthcare system a soft target for hackers to gain unauthorized access and steal crucial and sensitive information. Countries such as the UK and the US recently received such challenges, highlighting the need for effective data maintenance. IoT emerged as one of the critical solutions for data management systems in terms of addressing data security which certainly can enhance overall data collection, storage, maintenance, prediction of potential data security breaches and taking appropriate measurements. The concerned research considers a secondary data collection process where necessary data is collected from original scholarly articles, books and journals. Apart from that, a positivism research philosophy, a deductive research approach and a descriptive research design have been considered for this study. Qualitative data analysis techniques have also been incorporated into this research. Upon viewing the pros and cons of IoT algorithms, DES, AES, triple data encryption standards, and RSA encryption can be used in the healthcare system to facilitate data protection.

General Terms: Advanced Encryption Standard (AES), Data Encryption Standard (DES)

Keywords: IoT algorithms, data protection, data security, healthcare system, data management, cyberattacks.

ARTICLE INFORMATION

Author(s): Addanki Kavitha, B Srinivasa Rao, Dr Nikhat Akhtar, Dr Shaik Mohammad Rafi, Prabhdeep Singh, Dr Sunanda Das and Dr G Manikandan

Special Issue Editor: Dr. Sandeep Kautish
Received: 29/03/2022; **Accepted**: 21/04/2022; **Published**: 22/06/2022;
e-ISSN: 2347-470X;
Paper Id: 0222SI-IJEER-2022-04;
Citation: 10.37391/IJEER.100236
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100236.html

This article belongs to the Special Issue on **Novel Architecture and Methods in Industrial IoT and Wireless Sensor Network for Sustainable Computing**

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

The acquisition of data and the correct upkeep of that data appear to be the most critical factors for the modern healthcare system. Adequate data storage and maintenance allows the healthcare system to provide holistic patient care, increase communication with the medical team and provide more individualized treatment for each patient. This emphasizes the importance of adequate data collection and maintenance levels in the healthcare system, which is now lacking. On the other hand, data security challenges also occur with technological integration through various digital platforms [1]. Increased cyberattack threats emerged as one of the significant challenges healthcare faces in managing data and ensuring its adequate protection. Data security challenges become more meaningful for the healthcare system during Covid-19. Since the outbreak at the beginning of 2020, the virus has been accompanied by many cyber attackers looking for vulnerabilities in the data maintenance network within the healthcare system.

By launching ransomware assaults on hospitals, threats from organized cybercrime have fundamentally compromised data security [2]. An additional allegation made by the agencies is that hackers attempted to breach the safety of the Covid-19 research lab's computer systems. In the wake of the

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 270-275 | e-ISSN: 2347-470X

lockdown's adoption and the introduction of the virus, the world has begun to shift toward digital functioning, which includes healthcare services. Telemedicine and virtual therapy have developed as a new trend in the healthcare system, making the sector a potential target for cybercriminals and hackers. A spate of cyberattacks against national healthcare systems has been reported in several countries, including the United States, the United Kingdom, the Czech Republic, and others. Upon considering the prevalence of cyberattacks, the need for effective data security maintenance emerged as one of the key trends within the healthcare system [3].

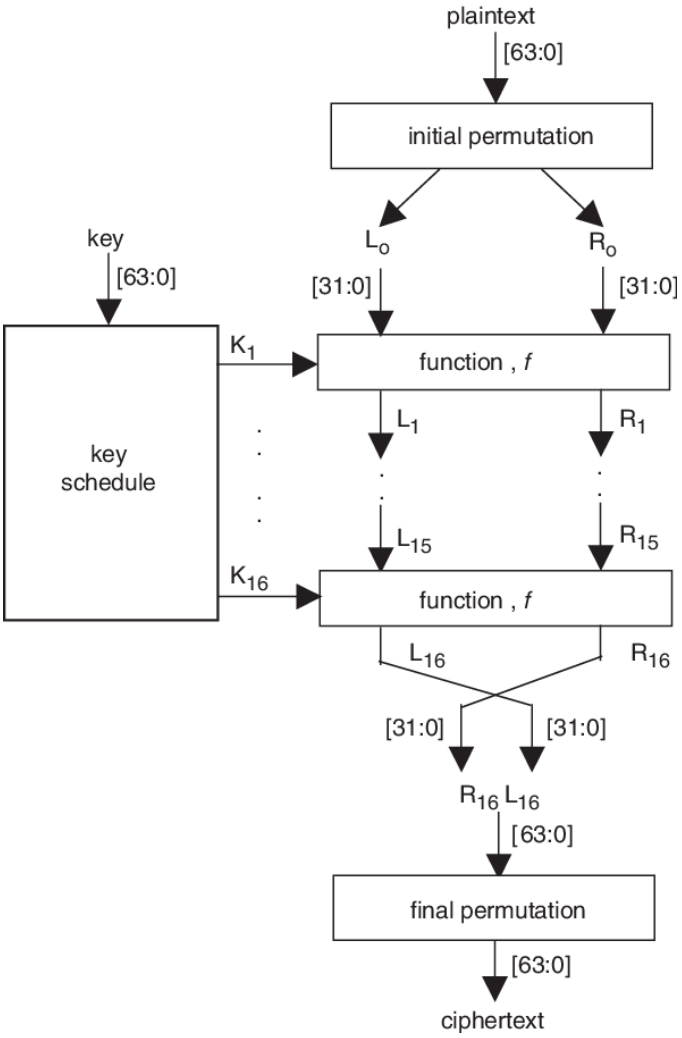


Figure 1: DES algorithm fundamentals
(Source: [4])

IoT appears to be one of the critical solutions to mitigate data protection and security challenges across different sectors. Specifically, for e-health devices, IoT emerged as a powerful application that certainly enhances eventual data security. IoT consists of sensors that collect data that is useful for consumers. Upon considering this factor, IoT is also used to protect data from potential cyber threats by utilising its full potential in addressing data security loopholes within the system. IoT sensors are mainly used to identify these loopholes and enhance data security within any sector [4]. "The Data Encryption Standard (DES)" appears to be one of the significant algorithms of IoT that essentially prevents potential data breaches within a system. It is a symmetric-key algorithm to ensure the encryption of digital data. On the other hand, data encryption is considered one of the effective ways to prevent potential data breaches and secure all types of data storage within a system. DES can avert possible attacks on the digital databases and ensure the data storage process upon viewing this factor. In addition, "Advanced Encryption Standard (AES)" is also considered an effective IoT algorithm that is used by several sectors to prevent potential data breaches through cyber-attacks [5]. On the other hand, "Triple Data Encryption Standard", "Twofish Encryption Algorithm", and "RSA Encryption" emerged as the necessary IoT algorithms used by several sectors across the world in terms of preventing data breaches and protecting data security.

2. LITERATURE REVIEW

Over the years, with technology dependence increased, threats from cyberattacks emerged as a significant challenge that certainly hampers the level of data security for the users. Moreover, Covid-19 emergence has further highlighted this challenge due to poor data security maintenance and increased cyberattacks. "Malware", "Phishing", "SQL injections", "Man-in-the-Middle (MIM) attacks", "Denial-of-Service (DOS) attacks", and "Password attacks" emerged as the most common yet effective cyberattacks that certainly cause compromised data security within a system [6]. On the other hand, ransomware attacks and DOS attacks appear to be significant cyberattacks witnessed by the healthcare system. These particular attacks directly hamper data security by hacking digital data sources. Apart from that, phishing and password attacks emerged as other relevant and significant attacks that compromise data sources within the healthcare system due to its lack of adequate protection.

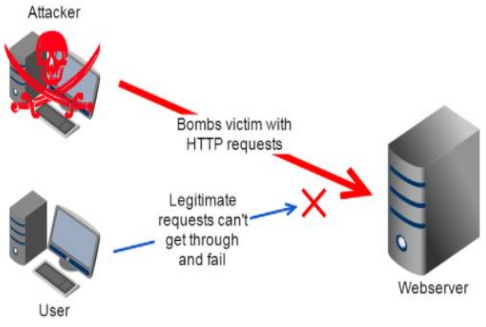


Figure 2: DOS attack fundamentals
(Source: [7])

Several countries, such as the US and the UK, have witnessed significant challenges related to data protection and data security violations within the healthcare system during Covid-19. Significant challenges such as database hacks, unauthorized access to sensitive patient data, and the stealing of Covid-19 research-related data have been observed in the world's healthcare system [7]. Countries such as the US and UK mostly witnessed malware, ransomware, phishing and

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 270-275 | e-ISSN: 2347-470X

password attacks in healthcare during Covid-19. The main aim of those cyberattacks was to gain access to central databases and steal information related to vaccination, Covid-19 research progress and sensitive patient data [8]. This highlights the significant challenges the concerned sector faces and the significance of data protection within the healthcare sector. On the other hand, facilities such as telemedicine and virtual treatment using digital platforms undoubtedly contributed to the increased cyberattacks across the world during the Covid-19 pandemic.

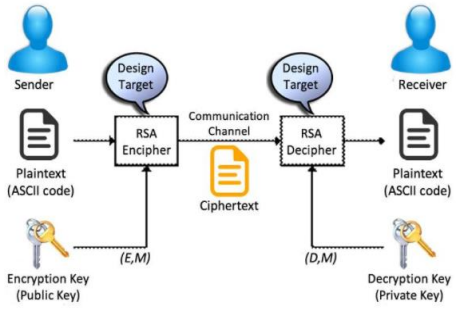


Figure 3: RSA structure
(Source: [9])

The need for adequate data protection and utilization of active technologies appears relevant in the current time. IoT is considered one of the most effective solution to data security challenges and ensures appropriate data collection. In-built sensors in IoT help effective data collection, which is further enhanced by the different algorithms to improve data security management [9]. The advanced encryption standard is considered as one of the most compelling IoT algorithms that essentially addresses data security challenges by ensuring early prediction of potential cyberattacks. AES uses keys of 192 and 256 bits for heavy-duty encryption, effectively secures data access and protects the network from possible collapse due to unauthorized access of malware. On the other hand, RSA encryption is an IoT algorithm used by modern computers to decrypt and encrypt messages [10]. It appears to be one of the significant alternatives healthcare systems can use to prevent significant data breaches and potential cyberattacks. It is public-key as "public-key cryptography" because it gives one key to the public and keeps one critical private.

3. METHODOLOGY

The search is based on ***secondary data*** to present comprehensive findings and enhance effective research outcomes. The main reason behind secondary data collection is its ability to quickly collect a wide range of data. Upon considering this aspect, the concerned research has collected necessary data on the type of cyberattacks faced by healthcare during Covid-19. On the other hand, ***positivism research philosophy*** integrates conducting scientific study and reaching effective outcomes. Considering this aspect, effective integration of the concerned research philosophy was integral in producing an objective-driven effect [11]. Identifying possible data patterns and trends is a significant advantage of positivism research philosophy. Applying this particular aspect, the concerned research ensured identifying necessary trends regarding cyberattacks in the healthcare system during Covid-19. In addition, a ***deductive research approach*** has also been undertaken in this research to conduct a logical analysis and enhance data generalization. This particular aspect has helped the concerned research incorporate efficient principles of providing a clear idea of concepts and variables, which happen to be one of the critical benefits of the deductive approach [12]. Moreover, the appropriate application of the reasoned approach also helped the concerned research with time-saving and produced an on-point discussion. Upon considering this particular aspect, the practical application of the reasoned research approach has allowed this study to outline concepts and variables and conduct thorough research on them.

A descriptive research design has been implemented to provide a systematic description of the phenomena and explain the experience during the study in the form of practical data analysis [13]. Moreover, the ability to conduct an in-depth analysis regarding the role of IoT algorithms in preventing cyberattacks appears to be another significant advantage provided by this particular research design. ***Secondary data*** for this research has been collected from authentic online sources. Major databases such as "Google Scholar" and "ProQuest" have been accessed to collect relevant scholarly journals for this research. In addition, online journals and websites have also been accessed to gather adequate information for the concerned study. The ***qualitative data analysis method*** has been used in this research to produce quality insights on the research topic. One of the significant advantages of the concerned data analysis technique is its ability to work as a content generator, facilitating the research outcome [14]. The concerned research presents data analysis and findings together using this particular data analysis method.

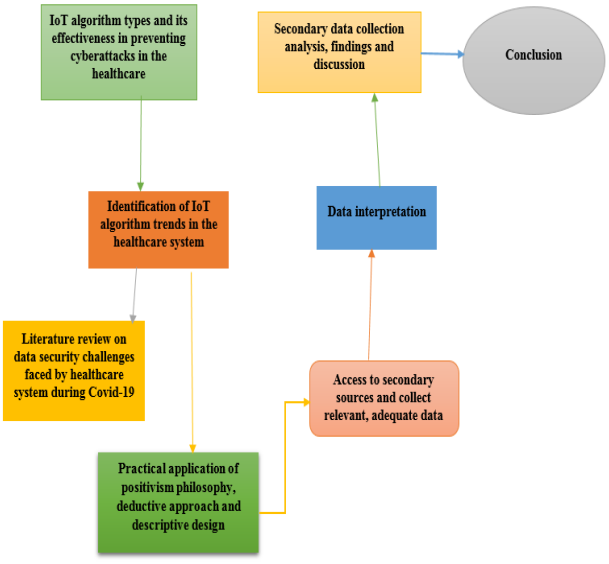


Figure 4: Flowchart diagram for the research

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 270-275 | e-ISSN: 2347-470X

4. ANALYSIS AND INTERPRETATION

The need for adequate data protection became more relevant during the Covid-19 outbreak due to the massive amount of cyberattacks across health institutions in the world. It has been observed that the lack of appropriate data protection systems and increased digital access essentially encouraged cyber attackers to launch online attacks on healthcare institutions [15]. Several countries such as the UK, the US, and the Czech Republic have witnessed such attacks and stealing of sensitive medical information. Patient data, Covid-19 vaccination data and research progress emerged as the essential data to be stolen by the hackers during the pandemic. Frequent attempts of data stealing and lack of adequate security emerged as the major concerns for the healthcare system during this time [16]. It is further believed that increased online medical activities such as telemedicine and digital treatment have certainly been the hackers' main targets in accessing sensitive medical information. Considering the contemporary healthcare system challenges, IoT algorithms appear to be one of the critical solutions to enhance data security within the healthcare system. The practical application of different IoT algorithms facilitates data security in the healthcare system differently. Primarily IoT is used for effective data collection, which enhances data analysis and predicts the potential trends in the healthcare sector [16]. IoT sensors play an influential role in data collection. However, this particular feature can further be utilized while predicting possible cyberattacks on the system. To ensure effective prediction regarding potential security threats, IoT algorithms are used to enhance tracking of the website health institutions are accessing along with the extent it is allowing access to external and dubious sources. IoT algorithms effectively predict potential data breach chances within the healthcare system and its probable solutions upon considering these data.

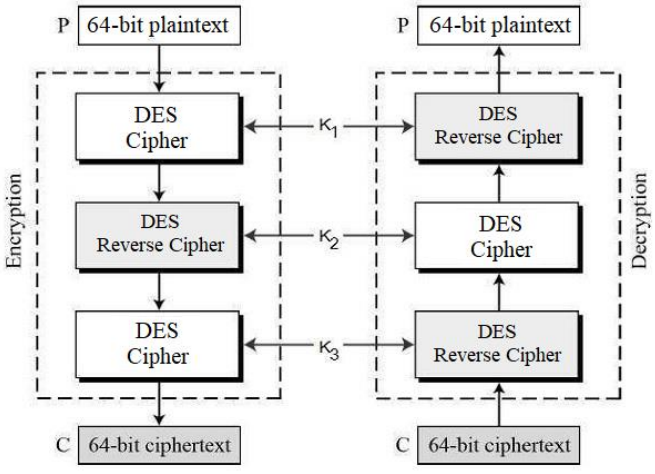


Figure 5: Structure of triple data encryption standard (Source: [17])

On the other hand, DES, AES, triple data encryption standards, RSA encryption and Twofish encryption algorithms appear to be powerful IoT algorithms used for data protection within the healthcare system. Effective implementation of the IoT algorithm further ensures that digital data is secured with end-to-end encryption, which can certainly be a probable solution to the identified data security challenges [17]. Upon considering this factor, the healthcare system can essentially implement DES and RSA encryption to enhance its data security, which can facilitate the eventual outcome of data management within the healthcare system. This can also ensure sensitive data security within the concerned sector and boost overall data protection by predicting and preventing potential data breaches. The AES algorithm is a symmetric block cypher that encrypts and decrypts the information, enhancing data security. It significantly converts data to an unintelligible form called "ciphertext". This also can be solved if needed. Upon considering this aspect, the precise role of IoT algorithms in enhancing data security within the healthcare system can be seen.

5. DISCUSSION AND FINDINGS

Over the years, digital data emerged as one of the major trends identified in healthcare in terms of maintaining solid databases and facilitating operations. Considering this aspect, effective data management emerged as the ultimate key to success for all industries worldwide. The emergence of Covid-19 has further increased the chances of utilizing digital platforms to ensure effective data management and communication with patients, doctors and other medical staff. Telemedicine and digital treatment appear to be key trends during the pandemic, which helped millions of people [18]. However, increased online activities emerged as critical reasons behind active cyberattack incidents within countries such as the US and UK. Healthcare emerged as the soft target for cyber attackers to conduct massive online attacks and gain access to sensitive information. Data related to confidential patient details, Covid-19 research progress and details about vaccination availability emerged as necessary targets for healthcare, which certainly created a collective threat for the health system in terms of securing sensitive medical information from hackers [18]. Further observed ransomware, malware attacks, password attacks, phishing and DOS emerged as the most common yet effective cyberattacks faced by the healthcare system, which essentially hampered healthcare data management. On the other hand, IoT algorithms emerged as an effective solution for the overall data management process in the healthcare system.

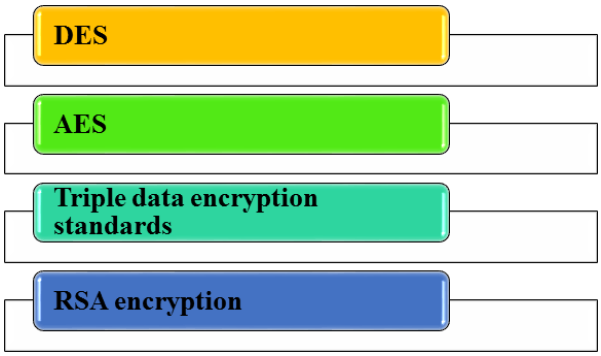


Figure 6: IoT algorithms to be applied in the healthcare system (Source: [18])

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 270-275 | e-ISSN: 2347-470X

Effective integration of IoT usually helps with appropriate data collection, which certainly considers data related to business trends, stakeholder expectations and essential market trends through IoT sensors [18]. The same can be used for effective data security purposes in predicting the potential cyberattacks and alerting the system about them. This, in turn, effectively can help the entire healthcare system to take appropriate measures to prevent potential cyberattacks in the healthcare system. Upon considering the pros and cons of the IoT algorithms DES, AES, triple data encryption standards, and RSA encryption emerged as the powerful IoT algorithms to enhance data security within the healthcare system. On the other hand, the appropriate application of necessary IoT algorithms can undoubtedly create a robust encryption system that is considered the eventual goal of maintaining adequate data privacy.

By considering the same purpose, Naïve Bayes Classifier based algorithm has been used in this research study through which the conditional probability can be calculated. The main advantages of such algorithm is that it is intractable due to which the intrusion in the computer can be detected easily. Hence, more security can be provided. In addition to this, bayes theorem also provides the principled ways for calculating the probability with conditions.

The simple form of the calculations for Bayes theorem is

P(A|B) – P(B|A) * P(A) / P(B)

P(A|B) : Posterior probability

P(yi | x1, x2, …, xn) = P(x1, x2, …, xn | yi) * P(yi) / P(x1, x2, …, xn)

The conditional probability of the observation based on the class *P(x1, x2, ..., xn | yi)* is not feasible unless the number of examples is extraordinarily large

Simplified or Naïve Bayes

P(yi | x1, x2, …, xn) = P(x1, x2, …, xn | yi) * P(yi)

In the next stages the conditional probability of the all the variables effectively changed into separate conditional probabilities. These independent conditional variables are also then multiplied together.

P(yi | x1, x2, …, xn) = P(x1|yi) * P(x2|yi) * … P(xn|yi) * P(yi)

In this research study a small example on a machine learning dataset has been derived below.

```
# example of generating a small classification dataset
# generate 2d classification dataset
X, y = make_blobs(n_samples=100, centers=2, n_features=2, random_state=1)
# summarize
print(X.shape, y.shape)
print(X[:5])
print(y[:5])
```

During the time of running this example, *"random_state"* is set to 1. Therefore, for each time same random sample of observation is generated for same random sample.

Hence, the input output elements of the first five example is

```
(100, 2) (100,)
[[-10.6105446    4.11045368]
 [  9.05798365   0.99701708]
 [  8.705727     1.36332954]
 [ -8.29324753   2.35371596]
 [  6.5954554    2.4247682 ]]
[0 1 1 0 1]
```

This numerical input variables are further modelled using ***Gaussian probability distribution.***

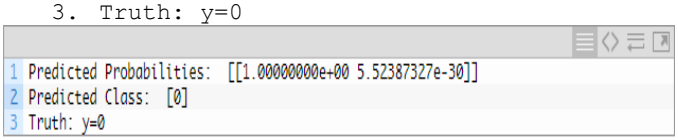
Example of Gaussian Naïve Bayes Model

INPUT

```
# example of gaussian naive bayes
from healthcare.datasets import make_blobs
from sklearn.naive_bayes import GaussianNB
# generate 2d classification dataset
X, y = make_blobs(n_samples=100, centers=2, n_features=2, random_state=1)
# define the model
model = GaussianNB()
# fit the model
model.fit(X, y)
# select a single sample
Xsample, ysample = [X[0]], y[0]
# make a probabilistic prediction
yhat_prob = model.predict_proba(Xsample)
print('Predicted Probabilities: ', yhat_prob)
# make a classification prediction
yhat_class = model.predict(Xsample)
print('Predicted Class: ', yhat_class)
print('Truth: y=%d' % ysample)
```

OUTPUT

```
Predicted Probabilities:  [[1.00000000e+00 5.52387327e-30]]
Predicted Class:  [0]
Truth: y=0
```



DES ensures that IoT thoroughly analyses potential data threats by considering a comprehensive evaluation of security breaches and facilitating data protection systems. On the other hand, RSA encryption essentially enhances data protection by ensuring maintenance of privacy and allowing the users to take effective control over information distribution and data security enhancement. RSA algorithms maintain data keys effectively by distributing one vital to the public and keeping one key private [18]. Effective maintenance of this process essentially provides appropriate data protection. AES 256 is considered one of the safest algorithms to protect data. Moreover, it is also easy maintenance that the modern

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 270-275 | e-ISSN: 2347-470X

healthcare system can use to facilitate data protection. Experts say AES might take several years to be broken by the hackers, mainly highlighting its effectiveness within the healthcare system. In addition, AES lasts longer than the IoT algorithms, making it a suitable fit in the healthcare system. RSA and AES, both IoT algorithms, are considered equally effective in protecting data and ensuring appropriate security in database systems. Upon viewing this aspect, the healthcare system can essentially use any of these algorithms to facilitate data protection and security enhancement.

6. CONCLUSION

With time and the rise of digital technologies, the need for effective data collection, storage and management emerged as crucial aspects for industries worldwide. Effective integration of digital technology during the Covid-19 pandemic helped numerous people avail of health facilities through telemedicine and digital treatment. However, this appears to be one of the critical reasons behind increased cyberattack challenges within the healthcare system. Considering this aspect, the need for the effective integration of IoT algorithms can be identified. IoT algorithms such as DES, AES, triple data encryption standards and RSA encryption can essentially enhance the data protection of the healthcare system at present.

REFERENCES

[1] Muthuppalaniappan, M. and Stevenson, K., (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, 33(1), p.mzaa117.

[2] Pranggono, B. and Arabo, A., (2021). COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), p.e247.

[3] He, Y., Aliyu, A., Evans, M. and Luo, C., (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of medical Internet research, 23(4), p.e21747.

[4] Jalali, M.S., Landman, A. and Gordon, W.J., (2021). Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association, 28(3), pp.671-672.

[5] Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, p.102248.

[6] Hijji, M. and Alam, G., (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. Ieee Access, 9, pp.7152-7169.

[7] Chigada, J. and Madzinga, R., (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23(1), pp.1-11.

[8] Nallainathan, S., (2021). Analysis onto the Evolving Cyber-Attack Trends during COVID-19 Pandemic. International Journal of Science and Research (IJSR), 10(4).

[9] Doyle, L., McCabe, C., Keogh, B., Brady, A. and McCann, M., (2020). An overview of the qualitative descriptive design within nursing research. Journal of Research in Nursing, 25(5), pp.443-455.

[10] Park, Y.S., Konge, L. and Artino, A.R., (2020). The positivism paradigm of research. Academic Medicine, 95(5), pp.690-694.

[11] Khan, N.A., Brohi, S.N. and Zaman, N., (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

[12] Abdulghani, H.A., Nijdam, N.A., Collen, A. and Konstantas, D., (2019). A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective. Symmetry, 11(6), p.774.

[13] Lachner, C. and Dustdar, S., (2019), June. A performance evaluation of data protection mechanisms for resource constrained iot devices. In 2019 IEEE International Conference on Fog Computing (ICFC) (pp. 47-52). IEEE.

[14] Kuzminykh, I., Carlsson, A., Yevdokymenko, M. and Sokolov, V., (2019). Investigation of the IoT device lifetime with secure data transmission. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems (pp. 16-27). Springer, Cham.

[15] Richards, K.A.R. and Hemphill, M.A., (2018). A practical guide to collaborative qualitative data analysis. Journal of Teaching in Physical Education, 37(2), pp.225-231.

[16] Woiceshyn, J. and Daellenbach, U., (2018). Evaluating inductive vs deductive research in management studies: Implications for authors, editors, and reviewers. Qualitative Research in Organizations and Management: An International Journal.

[17] Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A. and Yaqoob, I., (2017). Big IoT data analytics: architecture, opportunities, and open research challenges. ieee access, 5, pp.5247-5261.

[18] Torre, I., Koceva, F., Sanchez, O.R. and Adorni, G., (2016), December. A framework for personal data protection in the IoT. In 2016 11th international conference for internet technology and secured transactions (ICITST) (pp. 384-391). IEEE.