ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Data Analytics on Health Care Using IOT

Rishi keshav S[1], Priyanka S[2], Reshma C[3], SnehaVarsha Raj[4]

UG Student, Department of CSE, Sri Krishna Institute of Technology, Bengaluru, India[1].

UG Student, Department of CSE, Sri Krishna Institute of Technology, Bengaluru, India[2].

UG Student, Department of CSE, Sri Krishna Institute of Technology, Bengaluru, India[3].

UG Student, Department of CSE, Sri Krishna Institute of Technology, Bengaluru, India[4].

Abstract - We are entrenched in a new technological era. Emerging technologies like artificial intelligence (AI), neural networks, cloud computing, machine learning, deep learning, wearables, and Internet of Things (IoT) are redefining the way we have typically approached and navigated industries such as healthcare, automotive and more. Due to the significant advancement of the internet of things (IoT) in the healthcare sector, thesecurity and the integrity of the medical data became big challenges for healthcare services applications. Easy access to certain features and applications gave rise to the powerfulness and efficacy of various threats, risks and vulnerabilities that can victimize user's private data residing in smartphone paradigm.Therefore, a framework is required that facilitates collection, extraction, storage, classification, processing, and modelling of this vast heterogeneous volume of data. This paper proposes a healthcare big data framework through Data Analytics and Internet of Things (IoT). To better understand, and ultimately solve these big data challenges, data analysts can leverage two different perspectives: the data analytics (machine learning) framework and the IoT system framework.In order to secure the diagnostic text data in medical images, the proposed hybrid encryption schema is built using a combination of Advanced Encryption Standard (AES), and Rivest, Shamir and Adelman (RSA) algorithms.

KEYWORDS: Machine Learning, Internet of Things, Healthcare services and security, Smart devices.

I. INTRODUCTION

IoT creates an integrated communication environment of interconnected devices by engaging both virtual and physical world together. With the development of network-enabled sensors and artificial intelligence algorithms, various human-centred smart systems are proposed to provide services with higher quality, such as smart healthcare, affective interaction and autonomous driving, etc. The traditional healthcare system generates enormous amounts of patient data (medical records, images, videos, and ICU signals) every day. With the advent of remote digital healthcare based IoT systems, the transmission of medical data becomes a daily routine. Therefore, it is necessary to develop an efficient model to ensure the security and integrity of the patient's diagnostic data transmitted and received from IoT environment The rest of this paper is organised as follows: Section II presents the systematic review methodology. Section III presents the security to the model. Section IVconcludes the paper and gives future research directions.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

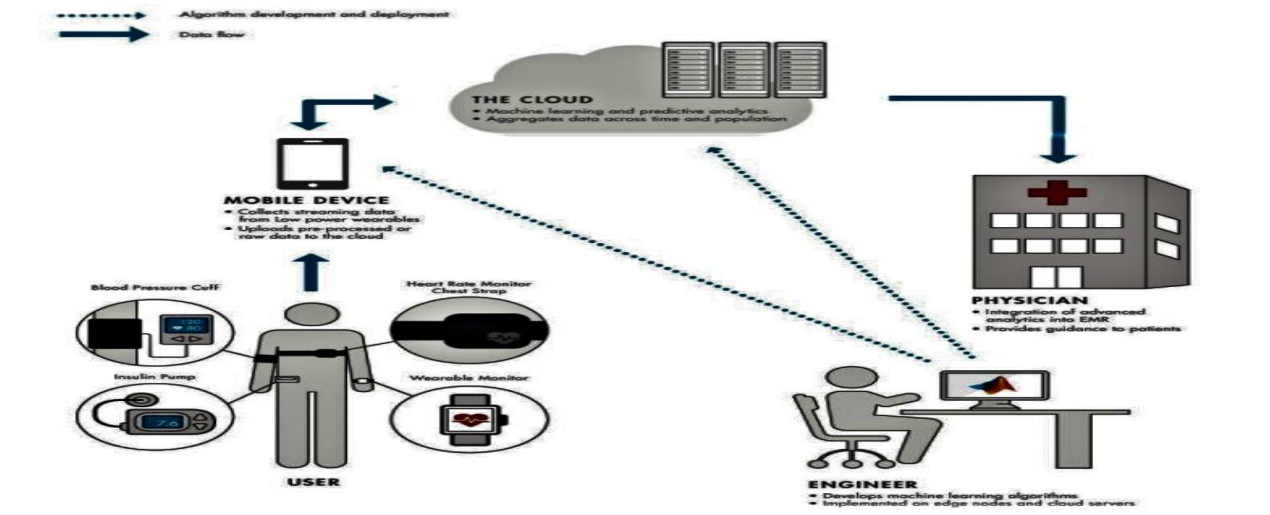
13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

II. METHODOLOGY

This paper proposes a healthcare big data framework through Data Analytics and Internet of Things (IoT).



A. Data Analytics View

The first framework that helps to better understand this changing landscape is the machine learning algorithm that adds intelligence into an entire system and helps transform data into actionable insights. Smart algorithms built using machine learning techniques enable the extraction of meaningful information from large amounts of text data, signals, images, and videos to automate and accelerate diagnostic capabilities.

A machine learning algorithm has three primary components:
1. Pre-processing of data
2. Feature extraction
3. Developing a predictive model

The training of the model is typically done on large amounts of historical data recorded over long periods of time using well established computational approaches. The trained model can then be applied on new, untested data to provide predictions on various parameters acting as an advanced diagnostic aid to the physician and/or patients.
Being able to prototype signal processing algorithms, while quickly exploring machine learning models and rapidly implement them on a target platform through C-code generation technologies is helping companies accelerate the development of such complex medical device products.

B. The IoT System View

The second framework that helps characterize digital health is the IoT system framework. An IoT framework typically has three main elements:
1. Edge node(s)
2. A gateway or a cloud aggregator
3. A back-end data analytics engine operating on the aggregated data for trend analysis, anomaly detection, etc.

Edge nodes typically collect raw physiological health data through various sensors. Wearable fitness devices as well as some proprietary FDA-regulated devices, such as blood glucose sensors and ECG monitors, are examples of edge

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

nodes in an IoT system. Data collected from the edge nodes needs to be processed to extract meaningful information from it.

With the right signal or image processing algorithms running on the sensor data streamed from the edge nodes, signal features can be extracted and transmitted to a cloud in a way that reduces bandwidth requirements and improves power efficiencies of these wearables that leads to reduced device size and longer times between recharges. The feature extraction algorithms may be run locally on the low-power embedded processor, which allows processed or compressed information to be sent to the cloud periodically, and then aggregated for a single patient or across a population of patients on the cloud. Predictive analytics can be run on the larger data collected across patients and time to provide patients and physicians with real-time reports.

III. SECURITY

With the rapidly expanding number of android devices, more new-fangled and creatively proceeded, subsequently tougher to elude, attacks are being launched on smart devices. A major part of such assaults is plausible because of the negligence of the end-users and clients. Without opposing the consequences of being under attack, the clients and end-users are struggling more to make the best out of their smart devices.

To develop an efficient model to ensure the security and integrity of the patient's diagnostic data, the data is encrypted using a proposed hybrid encryption scheme that is developed from both AES and RSA encryption algorithms. This goal is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image.

Cryptography is another term for data encryption. Cryptography encryption is the process of translating plain text data into something that appears to be meaningless (ciphertext),in a way that hackers cannot read it, but that can be authorized personnel. Decryption is the process of converting ciphertext back to plaintext. The two main algorithms used for data encryption in this work are the Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm.

AES is a symmetric cipher where the same key is used on both sides. It has a fixed message block size of 128 bits of text (plain or cipher), and keys of length 128,192, or 256 bits. When longer messages are sent, they are divided into 128-bit blocks. Apparently, longer keys make the cipher more difficult to break, but also enforce a longer encrypt and decrypt process.

On the contrary, the RSA is a public key algorithm, which is one of the most successful, asymmetric encryption systems today. It has the advantage of having a variable key size ranging from (2-2048) bits. As opposed to traditional, symmetric encryption systems, RSA works with two different keys: A public and a private one. Both work complementary to each other, which means that a message encrypted with one of them can only be decrypted by its counterpart. Since the private key cannot be calculated from the public key, the latter is generally available to the public.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Algorithm (1): Hybrid (AES & RSA) Algorithm.

Inputs: secret plain Stext message.

Output: main_cipher message , key s

Begin

1. Divide plain msg into two parts (Odd_Msg, Even_Msg)
2. Generate new AES key s
3. EncOdd = AES-128 (Odd_Msg, s)
4. Generate new RSA key (public = m) and (private = x)
5. EncEven = RSA (Even_Msg, m)
6. Build FullEncTxt by inserting both EncOdd and EncEven in their indices
7. EncKey = AES-128 (x, s)
8. Compress FullEncMsg by convert to hashs
9. Compress EncKey by convert to hashs
10. Define message empty main_cipher = ""
11. main_cipher = Concatenate (FullEncMsg, EncKey)
12. Return main_cipher and s

End

The security of RSA itself is mainly based on the mathematical problem of integer factorization. A message that is about to be encrypted is treated as one large number. When encrypting the message, it is raised to the power of the key, and divided with remainder by a fixed product of two primes. By repeating the process with the other key, the plaintext can be retrieved again. The best currently known method to break the encryption requires factorizing the product used in the division. Currently, it is not possible to calculate these factors for numbers greater than 768 bits. That is why modern cryptosystems use a minimum key length of 3072 bits.

Identifying the right combination of the algorithms for pre-processing and feature extraction is a critical step in this workflow and can determine the effectiveness of the final predictive analytics solution. It can also be difficult and time-consuming to figure out the right partitioning of algorithms without the right engineering and algorithm prototyping.

IV. CONCLUSION

In machine learning, a computer first learns to perform a task by studying a training set of examples. The computer then performs the same task with data it hasn't encountered before. This article presents a brief overview of machine-learning technologies, with a concrete case study from code analysis.

Data-driven analytics are pushing the boundaries of what's possible, especially in digital health. As healthcare regimes move towards more personalized medicine, it's likely that both preventative and therapeutic care will be driven by predictive analytics collected from wearables and shared on smartphones and personal devices. A key enabler of success in shifting systems will be engineering software tools, like MATLAB, that let medical device engineers and researchers prototype and implement advanced algorithms, analyse large amounts of varied types of data quickly and effectively, and develop/deploy new machine learning models without coding them from scratch, ultimately allowing for a better understanding of a patient's health and a more effective diagnosis of a wide range of human physiological conditions leading to a healthier society.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

REFERENCES

[1] M. Amiribesheli, A. Benmansour, and A. Bouchachia, "A review of smart homes in healthcare," Journal of Ambient Intelligence & Humanized Computing, vol. 6, no. 4, pp. 495–517, 2015.
[2] K. Hwang and M. Chen, Big-data analytics for cloud, IoT and cognitive learning, Wiley, U.K., ISBN: 9781119247029, 2017.
[3] S. Smalley, and R. Craig. "Security Enhanced (SE) Android: Bringing Flexible MAC to Android." In NDSS, vol. 310, pp. 20-38. 2013.
[4] "The Impact of Mobile Devices on Information Security: A Survey of IT and Security Professionals", October 2014. [Online]. Available: http://www.checkpoint.com/downloads/products/check-point-mobilesecurity-survey-report.pdf. [Accessed: June, 2016].
[5] Mandal, A. K., Parakash, C., & Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on (pp. 1-5). IEEE.
[6] Bashir, A., Hasan, A. S. B., &Almangush, H. (2012). A new image encryption approach using the integration of a shifting technique and the AES algorithm. International Journal of Computers and Applications, 42(9).
[7] Ashraf Darwish, Aboul Ella Hassanien, Mohamed Elhoseny, Arun Kumar Sangaiah, Khan Muhammad, The Impact of the Hybrid Platform of Internet of Things and Cloud Computing on Healthcare Systems: Opportunities, Challenges, and Open Problems, Journal of Ambient Intelligence and Humanized Computing, 2017 (https://doi.org/10.1007/s12652017-0659-1).
[8] Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Information Security Journal: A Global Perspective, 25(4-6), 197-212.
[9] Mare, S. F., Vladutiu, M., & Prodan, L. (2011). Secret data communication system using Steganography, AES and RSA. In Design and Technology in Electronic Packaging (SIITME), 2011 IEEE 17th International Symposium for (pp. 339-344). IEEE.
[10] Kumar, P., & Lee, H. J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 12(1), 55-91.
[11] Yehia, L., Khedr, A., & Darwish, A. (2015). Hybrid security techniques for Internet of Things healthcare applications. Advances in Internet of Things, 5(03), 21.