Research Article

Cyber Security Aspects of System for Time Synchronisation across National Communication Networks Using Cyber Physical Framework

Sushant Chamoli

Asst. Professor, Department of CSE (Computer sc)

GEHU-Dehradun Campus

Abstract: A unique approach based on developments in machine learning techniques has been developed to rapidly and accurately identify frequency anomalies in atomic clocks. The results of the tests show that compared to the innovation technique and the extrapolation approach, the innovative method has a higher detection potential for micro frequency flaws and a faster discovery time. The problems with Indian UTC have also been discussed. The continual addition of a leap second to UTC is a significant negative. A Cyber-Physical System (CPS) has been proposed for the national timing system to identify a difference in atomic clocks. There have also been extensive expressions of worry on the safety of CPS. We have also discussed time allocation and the CPS model. During the study, eight different atomic clocks were considered and compared to one another. High levels of accuracy and precision were found in the developed model, and it was suggested that the 7 th and 8 th clocks have values of 0.9310 and 0.9643, while the recall and f1-scores are higher with values of 0.9643 and 0.9643, respectively. This indicates that results will vary in the LSTM based ML models of anomaly detection as epochs and noise levels vary.

Keywords: Cyber-Physical System (CPS), extrapolation, machine learning algorithm, f1-scores

Introduction

Coordinated Universal Time (UTC) is the standard by which civil time and international transmissions are measured. The internet uses many time protocols and the Global Positioning System (GPS) in addition to radio time signals and services offered by the national interacting clock. It's the basis for anything that requires knowing the time, whether on a global, regional, or national scale. The coordinated global time production demonstrates that determining global time is more complicated than just reading off the time from the globe. Still, it's the act of integrating and adapting several conceptual frameworks and methods of timing. Coordinated Universal Time (UTC) is the time reference used by the vast majority of the world's population. Coordinated Universal Time is the best method for tracking precise time. Coordinated Universal Time is based on the hours, minutes, and seconds of daylight at the prime meridian of Earth, which is about around Greenwich. Coordinated Universal Time is the standard by which time, frequency, and duration are expressed. Clocks all around the globe should show the same amount of minutes, seconds, and hours, and coordinated global time makes this possible. In terms of precision, frequency, and time interval measurements, the signals generated by oscillators that are synchronised to universal time are the gold standard. The term "Coordinated Universal Time" (sometimes known as "Lab Time") comes from the practise of synchronising clocks with astronomical observations. The official designation was announced in 1963 by the Consultative Committee on International Radiocommunications (CCIR). Coordinated Universal Time (UTC) is the standard by which civil time and international transmissions are measured. The internet uses many time protocols and the Global Positioning System (GPS) in addition to radio time signals and services offered by the national interacting clock. It's the basis for anything that requires knowing the time, whether on a global, regional, or national scale. The coordinated global time production demonstrates that determining global time is more complicated than just reading off the time from the globe. Still, it's the channel via which many conceptual frameworks and methods of time estimate may be communicated and combined. Coordinated Universal Time (UTC) is the time reference used by the vast majority of the world's population. Coordinated Universal Time is the best method for tracking precise time. Coordinated Universal Time is based on the hours, minutes, and seconds of daylight at the prime meridian of Earth, which is about around Greenwich. Coordinated Universal Time is the standard by which time, frequency, and duration are expressed. Clocks all around the globe should show the same amount of minutes, seconds, and hours, and coordinated global time makes this possible. In terms of precision, frequency, and time interval measurements, the signals generated by oscillators that are synchronised to universal time are the gold standard. The term "Coordinated Universal Time" (sometimes known as "Lab Time") comes from the practise of synchronising clocks with astronomical observations. The official designation was announced in 1963 by the Consultative Committee on International Radiocommunications (CCIR).

Framework of Cyber-Physical System For National Timescale System (Coordinated Universal Time (K))

The basic objective of CPS is to enable cooperation across the virtual and real worlds. They use software and technology to bridge the gap between the virtual and the real. The network of the cyber-physical system may evolve, adapt, and collaborate thanks to the incorporation of embedded technology linked to the physical environment through actuators and sensors. They are, however, bolstered by the realisation that physical achievements cannot be achieved without the incorporation of computation, sensing, actuation, and networking. A cyber-physical system is characterised by the integration of many systems and the use of cutting-edge technology. As a result, cyber-physical systems stretch the limits of integration, design-system design, and validation/verification in several ways. This places heavy demands on all parties engaged due to the need to exchange information and create across numerous areas, disciplines, technologies, and factors. Integration into a larger scale CPSoS (Cyber-Physical System of Systems) that is continuously performed, managed, and improved raises the bar for dependability in terms of security, reliability, safety, etc. Cyber-physical system development, design, and operation need grounded, scientifically validated methodologies that enable the interaction and composition of sub-parts with respect to legacy components and non-functional system demands. Public Working Group CPS framework has recognised the interconnection of systems, devices, people, and SoS from its inception by NIST in Cyber-Physical Systems. Furthermore, it determines the course of at least one decision-related activity or data flow. Here, data flow is a digital indication, but everything that happens is happening in the actual world.

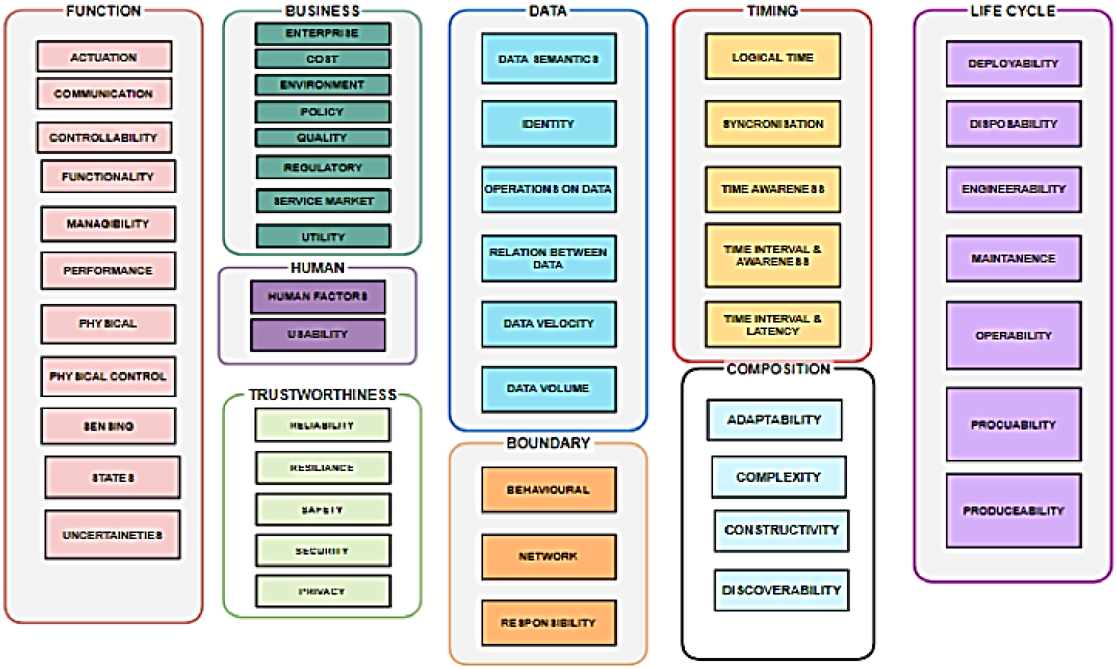


Figure 1 CPS Framework

Coordination on scales from the neighbourhood to the country to the world to the city is made possible through this. Supervising systems that feed information to regional control units and control units are crucial to the development of Smart Timescale Systems, but handling them delicately is essential. Information on the asset's measurement and functionality is given, and the environment's support system demonstrates the asset's optimal function condition. A smart timescale system is one in which the time scale system is enhanced by the flow of information and all processes within the framework of a cyberphysical system, rather than by the generation of qualities that are superior to its amount. Integrating information gathered in cyber and real-world settings will result in a deeper understanding of the state's affairs. Accurate timekeeping, smart energy management, and routine maintenance are all targets of this window of opportunity. See below for a schematic depiction of the Smart Global Timescale System's CPS architecture: In order to learn the SoS that is crucial to its functioning, and to use it in an iterative fashion to help with management. These advancements in sensing and computation allow for smarter and better behaving systems. Also, each module of the framework has to be considered when defining tools that use standardised service/component definitions, catalogues, and description components. Last but not least, it has to be made extensible by the incorporation of external interoperability and internally scalable components, which will benefit all applications and the provided domain. In the cyber-physical system, the system involving time scales (Coordinated Universal Time (k)) is one of the essential scientific fields. The global reference time is used as a crucial input source for a variety of real-time communication activities. Within its own infrastructure, the National Time Scale is dependent on communication between cyber and physical systems.

Literature Review

According to Ashibani and Mahmoud (2017), Active and passive security risks coexist. The goal of an active attack is to alter the system's behaviour by the attacker while they have control of it. Passive attacks are famously difficult to detect because of the time it takes for the attacker to get access to the information without interrupting the functionality of the system. CPS faces two major categories of security threats: Both interlayer and intralayer threats exist.

Perception Layer: It's also known as the recognition layer or the sensing layer (Mahmoud et al., 2015). Sensors, actuators, aggregators, radio frequency identification tags, global positioning system receivers, and many other devices fall under this category. These devices track, monitor, and make sense of their surroundings in real time by collecting data from them. 22 These sensors operate in both wide-area and local networks, providing the application layer with real-time data for analysis.

Transmission Layer: The second tier of the CPS architecture (Khan et al., 2012) is also known as the transport layer or the network layer. This layer performs data processing and communication between the perception and application layers. Bluetooth, 4G and 5G, InfraRed (IR) and ZigBee, Wi-Fi, Long Term Evolution (LTE), and a plethora of other LANs and communication protocols are used to carry data and promote interaction over the Internet. One such protocol is Internet Protocol version 6 (IPv6), which is used to support the ever-increasing variety of devices that may connect to the internet. Layer 2 infrastructure includes things like cloud servers, routers, switches, internet gateways, firewalls, and intrusion detection and prevention systems (IDS/IPS).

Application Layer: This third and final layer is the most dynamic of the bunch. After analysing the information gathered by the data transmission layer, this layer issues instructions to physical equipment such sensors and actuators to carry out (Gao et al., 2013). To achieve this goal, the collected data is fed into complex decision-making algorithms. This layer also receives information from the perception component and processes it to determine what predetermined actions to execute. In fact, cloud computing, middleware, and data mining techniques are used at this level of data management. Confidentiality requires that sensitive information be shielded from prying eyes. A strong multi-factor authentication solution is necessary at this tier to prevent unauthorised access and privilege escalation.

Research Methodology

The current investigation is firmly grounded on the experimental approach of the scientific method. Here, we detail the procedures we used to answer our research questions via data collection. A hypothesis, a possible research variable, and additional variables that may be investigated, measured, and compared are common components of the study design section. The most important thing is to do the studies in a controlled setting. The experiment's goal is to examine the effects of varying the experimental variable on the dependent variable. Before choosing whether or not to accept the study's hypothesised outcomes, the researcher will typically gather the relevant data. Sometimes called a "hypothesis testing" or "empirical research" technique. Every scientific study is designed to find some kind of link between two variables (the dependent and the independent). An experiment's outcomes may either support or refute a hypothesis concerning an object's correlation with an independent variable.

Machine Learning Algorithm

Some examples of algorithms that may be developed for ML-based architectures include K-Means, kNN, Random Forest, Logistic Regression, Linear Regression, Decision Tree, Naive Bayesian Bayes, and Support Vector Machines. Some examples of ML tasks that may be performed in Python include regression, clustering, classification, and anomaly detection. The data analysis for the developed model is performed using ML with Python with a focus on anomaly identification. The approach relies on a comparison of actual and projected outcomes, which are established by injecting a point abnormality into the original dataset of the system, in order to uncover and present anomalous datasets. The following flowchart outlines the steps used in the research to identify and illustrate inaccuracies.

The steps of the algorithm are explained below briefly:

The initial stage in identifying anomalies is inputting the irregular data and replacing the missing data with a point determined from the slope. This method is essential because anomalous data sometimes represents shifts in technical difficulties or other aberrations from typical behaviour. When outliers or missing values are found, the following stage is data imputation, which entails filling in the gaps. On the basis of the sequence anticipated by the model or the anomalous data, the time points that comprise the anomalies or missing values are identified. To close the data gaps, a linear fit was made to the existing data. Each pair of missing coordinates was connected by drawing a straight line.

The second step entails plotting the exact data in a time range of 0.3 to 0.5 seconds using point anomaly. Since point anomalies are often the simplest to identify, they have been the subject of many anomaly detection research. A point anomaly is a time interval that exceeds the standard accuracy of an atomic clock.

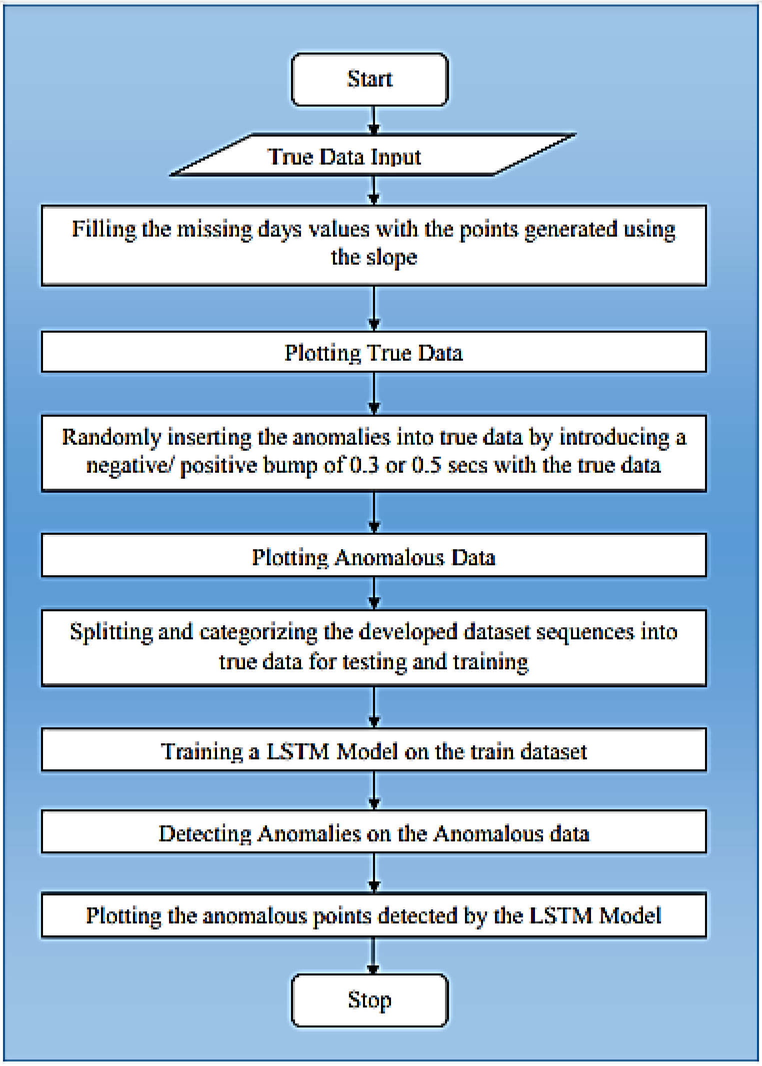

Start
True Data Input
Filling the missing days values with the points generated using the slope
Plotting True Data
Randomly inserting the anomalies into true data by introducing a negative/ positive bump of 0.3 or 0.5 secs with the true data
Plotting Anomalous Data
Splitting and categorizing the developed dataset sequences into true data for testing and training
Training a LSTM Model on the train dataset
Detecting Anomalies on the Anomalous data
Plotting the anomalous points detected by the LSTM Model
Stop

Figure 2 System Flow Chart of the Developed Model

Experimental Results

In the investigation, "anomalies detection" was utilised to spot inconsistencies in the data collected from eight separate atomic clocks. The recommended model has been tested and trained using just one set of data.

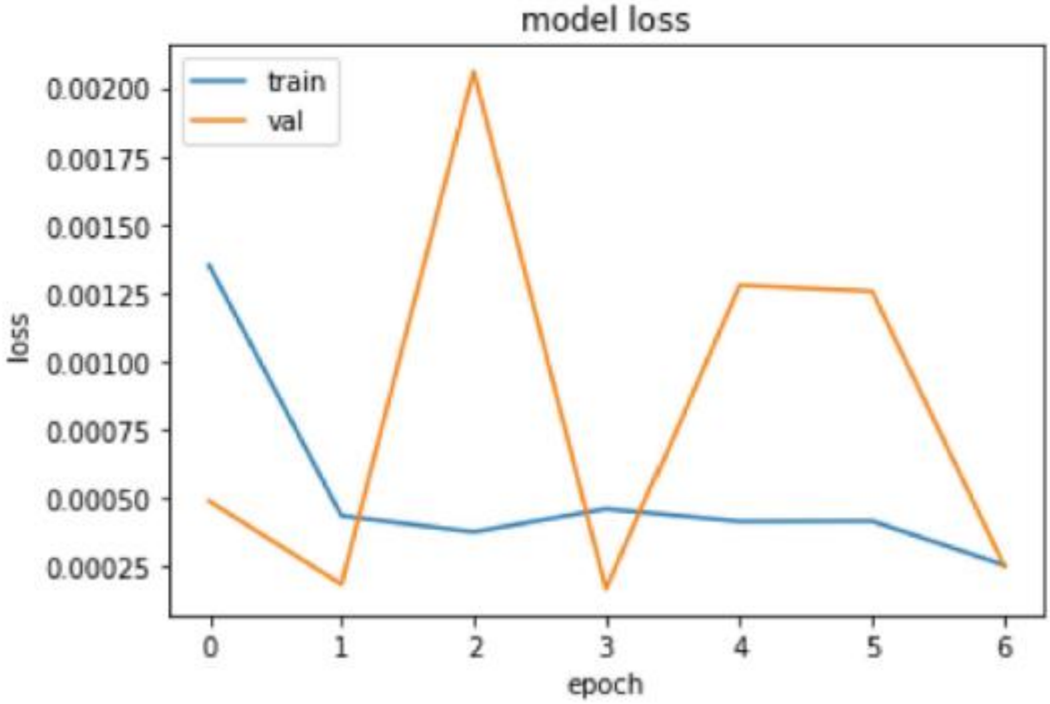
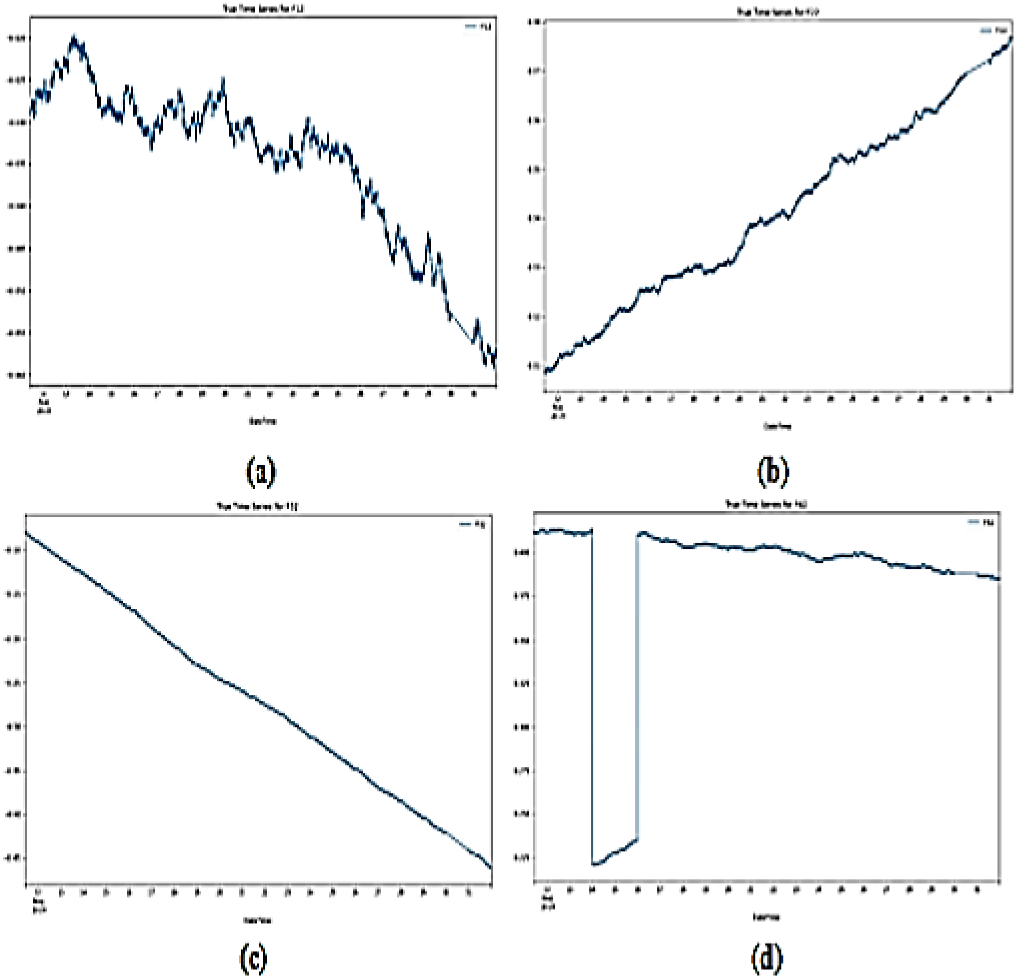


Figure 3. Model Loss Plot

Inference Increasing the number of CNN layers in the suggested design may help minimise validation errors, since validation loss seems to be higher than training loss in the preceding graph. The loss indicates how inaccurately the model anticipated a given case. The picture depicts the best loss curve to train a model employing ML techniques. In order to reduce validation loss and improve matching, additional CNN layers were added to the study. Furthermore, time-series data are used to assess the model's accuracy and efficiency.

Time Series before Adding in Anomalies

The below figure shows “before and after” injecting the point anomalies:



(a) (b) (c) (d)

Figure 4. (a) True Time-Series for August-September 2019: (a) F12, (b) F22, (c) F32, (d) F42

Performance Evaluation

Results for all eight clocks are shown in Figure 5; this includes precision, recall, accuracy, and F1-scores. Clocks 7 and 8 with higher values show more perfection and accuracy after all anomalies have been added, whereas Clocks 1 through 6 with lower values show the pposite.

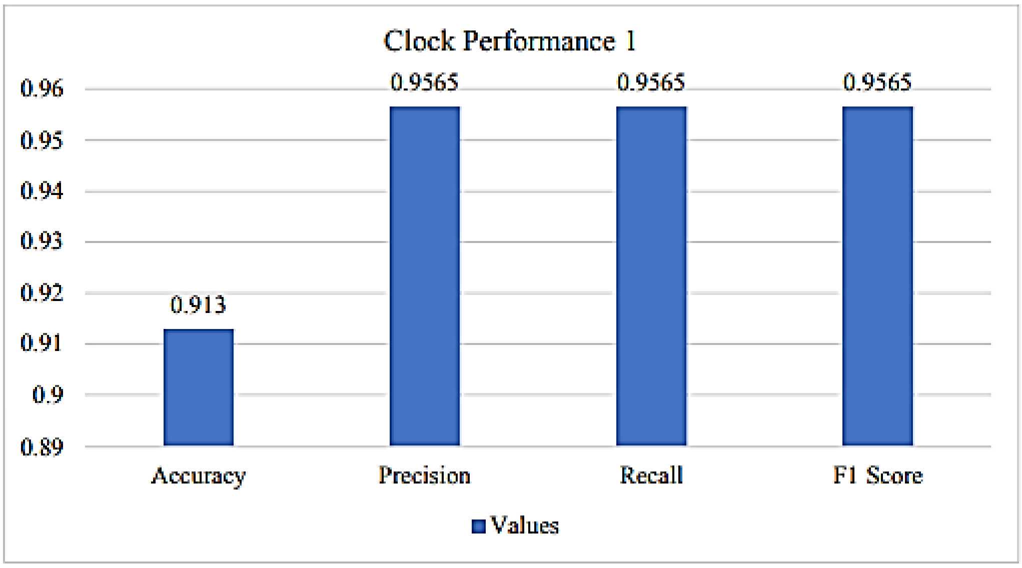


Figure 5. Clock Performance 7

Figure 5 displays the values of accuracy, precision, recall, and F1 Score. Precision, recall, and F1 are all calculated to be 0.9565, while accuracy is calculated to be 0.9130.

Figure 6: Value of F1 Score for Clock Accuracy, Precision, and Recall

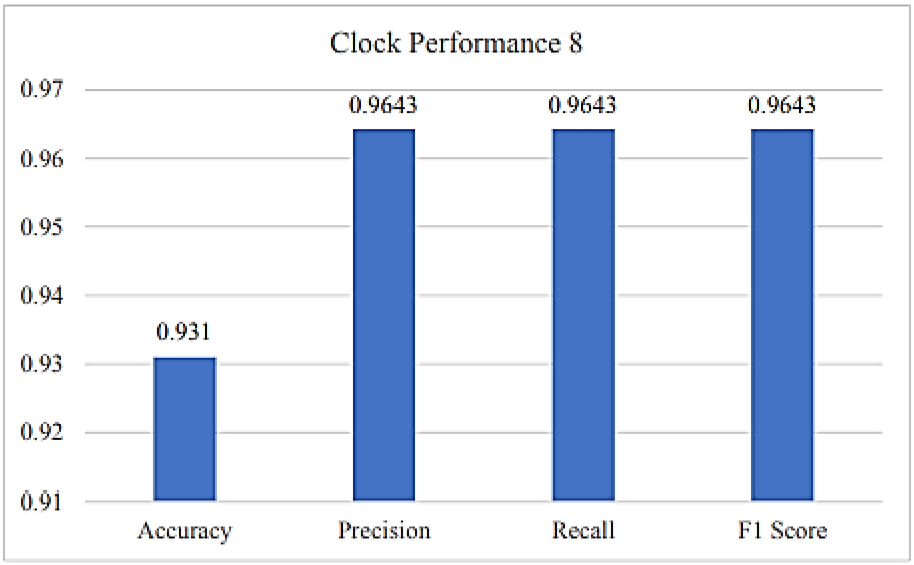


Figure 5 Clock Performance 8

Conclusion

The graphs demonstrate that the point anomalies discovered using the deep learning (DLAD) technique with the LSTM as the NN architecture is successful in detecting instances of wrong or faked data with greater accuracy and precision. Anomaly scores, network architecture development, and data as inputs are only a few of the methods used to find irregularities in the existing system. In this section, we also compare the precisions, accuracy, F1, and recall value that were achieved. At last, we compared the original datasets to anomalous point datasets to assess how well the proposed model performed. With values of 0.9310 and 0.9643 for accuracy and precision, respectively, the seventh and eighth clocks demonstrated greater performance, demonstrating that the developed model is a good fit. Results will vary between epochs and noise levels, however LSTM-based anomaly detection ML models had higher recall and f1-scores (0.9643 and 0.9643, respectively).

References

1. Agrawal, S, Jain, S & Sharma, S 2011, 'A survey of routing attacks and security measures in mobile ad-hoc networks' arXiv preprint arXiv:1105.5623.
2. Ahmad, S, Lavin, A, Purdy, S & Agha, Z 2017, Unsupervised Real-time Anomaly Detection for Streaming Data. Neurocomputing, volume 262,pp. 134–147.
3. Ashibani, Y & Mahmoud, QH 2017, 'Cyber physical systems security: analysis, challenges and solutions', Comput. Secur., vol. 68, pp. 81–97
4. Ashibani, Y & Mahmoud, QH 2017, 'Cyber-physical systems security: Analysis', challenges and solutions. Computers & Security, vol. 68, pp. 81-97
5. Ashibani, Y & Mahmoud, QH 2017, 'Cyber-physical systems security: Analysis, challenges and solutions', Computers & Security, vol. 68, pp. 81-97
6. Baeza-Yates, R & Ribeiro-Neto, B 2011, 'Modern Information Retrieval: The Concepts and Technology behind Search (Second Edition). Addison-Wesley',
7. Baskar, R, Raja, K, Joseph, C & Reji, M 2017, 'Sinkhole Attack in Wireless Sensor Networks-Performance Analysis and Detection Methods', Indian Journal of Science and Technology, vol. 10, no. 12, pp. 1-8.
8. Davis, JA, Shemar, S & Whibberley, P 2011, 'A Kalman filter UTC(k) prediction and steering algorithm', IEEE Publications
9. Gao, H, Peng, Y, Jia, K, Dai, Z & Wang, T 2013, 'The design of ICS testbed based on emulation, physical, and simulation (EPS-ICS testbed)', Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing IEEE 2013, pp. 420–423
10. Khan, R, Khan, SU, Zaheer, R & Khan, S 2012, 'Future internet: the internet of things architecture, possible applications and key challenges', 10th International Conference on Frontiers of Information Technology, IEEE 2012, pp. 257–260
11. Krishna PV, Saritha V & Sultana P 2015, 'Security issues of CPS, Challenges', Opportunities and Dimensions of CPS, pp 140-160
12. Ly K & Jin Y 2016, 'Security Challenges in CPS and IoT: from End Node to the System', IEEE Computer Society Annual Symposium on VLSI.
13. Mahmoud, R, Yousuf, T, Aloul, F & Zualkernan, I 2015, 'December. Internet of things (IoT) security: Current status', challenges and prospective measures', In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE
14. Mahmoud, R, Yousuf, T, Aloul, F & Zualkernan, I 2015, 'Internet of things (IoT) security: current status, challenges and prospective measures', 10th International Conference for Internet Technology and Secured Transactions (ICITST) IEEE 2015, pp. 336–341
15. Önal, C & Kirrmann, H 2012, 'Security improvements for IEEE 1588 Annex K: Implementation and comparison of authentication codes,' 2012 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), pp. 1-6.
16. Peng, Y, Lu, T, Liu, J, Gao, Y, Guo, X & Xie, F, 2013, 'October. Cyberphysical system risk assessment', In 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 442-447). IEEE
17. Tournier, J & Goerlitz, O 2009, Strategies to Secure the IEEE 1588 Protocol in Digital Substation Automation" Fourth International Conference on Critical Infrastructures (CRIS), pp. 27-30.

18. Wang, EK, Ye, Y, Xu, X, Yiu, SM, Hui, LCK & Chow, K.P., 2010, December. Security issues and challenges for cyber-physical system. In 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing (pp. 733-738). IEEE
19. Xu B, He J & Zhang L 2013, ‘Specification of Cyber-physical Systems Based on Clock Theory’, International Journal of Hybrid Information Technology, vol. 6, no. 3, pp. 45-53
20. Zhao, K & Ge, L 2013, ‘A survey on the internet of things security’, In 2013 Ninth international conference on computational intelligence and security (pp. 663-667). IEEE.