Security in Cyber-Physical Systems

Joanita Dsouza[1], Laura Elezabeth[2], Ved Prakash Mishra[3], Rachna Jain[4]

[1,2,3,4]*Amity University Dubai, UAE*

[1]*joany.dsouza98@gmail.com,* [2]*lauraeliza888@gmail.com,* [3]*mishra.ved@gmail.com*

Abstract: In this manuscript, we explore the network and cyber security challenges furthermore, issues of cyber or digital physical frameworks. (1) We epitomize the general work process of cyber or digital physical frameworks, (2) identify the conceivable vulnerabilities, assault issues, foes qualities and an arrangement of difficulties that are required to be addressed. A framework has been proposed for setting situation- apprehensive security structure for general digital or cyber physical frameworks with the implementation of biometrics.

Keywords: Cyber frameworks, security, Context-aware, biometrics.

I. INTRODUCTION

Cyber-Physical System (CPS) focuses at watching the behavior of physical procedures, and impelling activities to variation its behavior consequently making the physical condition work exactly and healthier. As a general rule, CPS comprises of two driving peripherals, a physical procedure and a digital framework. Constantly, the physical process is examined or powered by the digital framework, which is a sorted out arranged element of grouped minor gadgets with detecting, processing and correspondence (regularly remote) capabilities 1, 2]. CPS contribute to add to the factor of tight coupling between physical and programming segments. CPS can take part in diverse spatial and transient scales and showing various and near social modalities. Also, CPS are over and over converging with outside physical world, subsequently the actions of a CPS may fluctuate with the operative or ecological setting [2]. The physical procedure may incorporate checking security and developments of travelers in an open transport framework, or of vehicles on a street system or observing wellbeing and prosperity of domesticated animals and raising programmed alerts of ailments or wounds or the mix of both. In any case, as the physical and cyber frameworks connections increment, the physical frameworks are exceptionally subject to the vulnerabilities with respect to the security in the digital framework. There are different instances of programmers hacking into airport regulation [3], breaking of data in MyFitnessPal app, bargaining usernames, email, and passwords from the application's around 150 million client. Although at present, there are only few hackers who can hack the devices that are medically implanted into the human body as they have wireless communications [4]. Reports demonstrate that programmers have additionally broken into power frameworks in different spots [5] and furthermore equipped for messing with the elements of a moving vehicle [6] and instruments stretch incorrect readings by checking correspondences between the electronic control units (ECUs) and embed counterfeit bundles of information to do assaults. Presently programmers have made a virus which can effectively assault Siemens plant-control framework [7].

Despite the fact that, the vulnerabilities in security are being found basically in electronic power matrices, shrewd transportation frameworks, and medicinal frameworks, etc which are the digital physical frameworks. Subsequently, specialists are worried about the security of CPS. While building a more brilliant and exceptionally sure digital physical framework, we should check for the conceivable vulnerabilities on these frameworks and think about them. Digital physical frameworks security is another territory and very little creation has been done.[8] The amount of digital strikes is taking off. Reliably, there are 3,000 undertakings to enter the German national government's framework alone. Moreover, more undermining than the sheer volume of ambushes is their growing quality and multifaceted nature.

II. CYBER-PHYSICAL SYSTEM (CPS)

The customary working of a Cyber-Physical System has 4 main steps: Monitoring, Networking, Computing and Actuation.

A. Monitoring

- Basic function of CPS.
- Assess and provide feedback on previous actions.
- Ensure proper working on future actions.

B. Networking

- Deals with data aggregation and diffusion.
- CPS sensors can generate real time data. CPS contains many such sensors therefore data thus accumulated can be aggregated or diffused for processing by analyser.
- Networking communications enables simultaneous interaction of different applications.

C. Computing

- Analyses data generated during monitoring.

978-1-5386-9346-9/19/$31.00 ©2019 IEEE

- Ensures that pre-set criteria are met by the physical processes.
- If criteria not met, remedial measures are proposed and executed.

D. Actuation

- Executes actions determined in computing phase.
- Actuate various forms of actions including correcting the cyber behaviour of the CPS, changing the physical process.

Workflow of Cyber-Physical System is shown in Fig. 1.

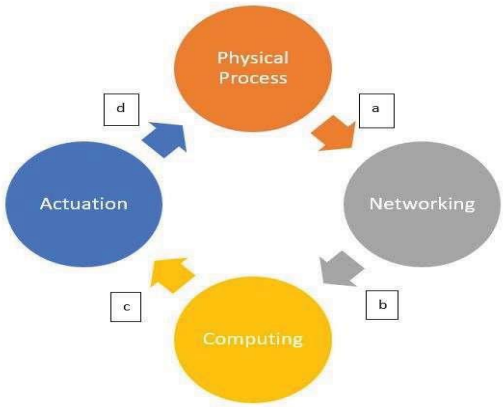

Fig. 1. Workflow of CPS [1].

Where,

a== data acquisition from sensors

b== physical data collection in-network

c== computed result

d== instructions shown to the actuators for control.

III. CYBER-PHYSICAL SYSTEM SECURITY

CPS security objectives are as follows:

A. Integrity

Integrity ensures data or assets can't be adjusted without approval. Integrity is damaged when an intruder unintentionally or with malevolent purpose alters or erases imperative information; and after that the recipients get false information and trust it to be valid [9].

B. Availability

High availability of CPS means to continuously give services by counteracting processing, controls, correspondence defilements because of equipment failure, control blackouts or up gradation of systems [10].

C. Confidentiality

Confidentiality means capability to prevent unauthorized individuals or systems from accessing information [11-12].

D. Authenticity

In communication and computing process it is important to guarantee that the information, exchanges, interchanges are bona fide. It is additionally essential for genuineness to approve that the two parties included are who they guarantee they are.[13] In CPS, the legitimacy expects to acknowledge confirmation in all the related procedure, for example, detecting, interchanges, incitation's.

IV. POTENTIAL AREAS AND TYPES OF ATTACKS ON CPS

A. Eavesdropping

Eavesdropping is the type of attack which is passive and the attacker can intercept information from the system [14]. CPS is extremely vulnerable to eavesdropping. Eavesdropping violates user's privacy.

B. Man-in-the-middle attack

This can appear as a false negative or a false positive which leads to problems such as performing of unrequired action or not performing the required action [15].

C. Denial-of-Service Attack

Sometimes legitimate requests for network resources are prevented from being processed. This type of network attack is called Denial of Service (DoS) attack [16]. This kind assaults for the most part transmits a gigantic measure of information to the system therefore making it occupied in taking care of the information with the goal that typical administrations cant be even. To put it plainly, the refusal of benefit assault prevents ordinary work or even utilization of framework. The attacker can access the system of digital physical frameworks and can surge a controller connect with activity until the point that a shutdown occurs due to over burden or send information which is invalid to the framework which prompts irregular end or can square movement which results in lost access.

V. CYBER-PHYSICAL SYSTEMS SECURITY MODELS

For risk assessment and management for CPSs, following 5 models are popular.[17].

A. Expert Elicited Model

This technique includes computational models to survey risk dependent on master inspired identification and portrayal of cyber system traits, for example, organize information streams and the estimation of the weakness of those assets and

information streams to various kinds of compromise. One noteworthy disadvantage of this methodology is absence of completeness [17].

B. Attack Graph

This methodology has numerous merits. Central is a light information necessity. Models in this class don't endure exactness or constancy weaknesses since they are developed straightforwardly from framework information without reflection or accumulation. Another favourable position of this methodology is adaptability [17].

C. Game theoretic model

This model unequivocally speaks to the correspondence of assailants and shields in a theoretic framework. Models are essentially more shifted and the procedure is considerably less created than the master evoked [17].

D. Petri Net models

Using the Petri net graph, a digital assault is demonstrated as the progressive exploitation of vulnerabilities on hosts to heighten and after that misuse benefits on the system [17].

E. Stochastic games

This strategy incorporates stochastic games on Petri nets, making a significantly more unfathomable and furthermore difficult approach. This model propels subject to assaults contrasting with the system monitor measures displace misuse explicit advances [17].

Security models can be helpful for assessing hazard and for different other security estimations. Metrics are portrayed as quantifiable properties of a framework that assess how much focuses of the framework are practiced. Metrics can outfit digital defenders of a CPS with essential encounters concerning the structure. Metrics are generally picked up by dissecting material qualities of that particular system.

VI. CONTEXT-AWARE BIOMETRIC SECURITY FRAMEWORK

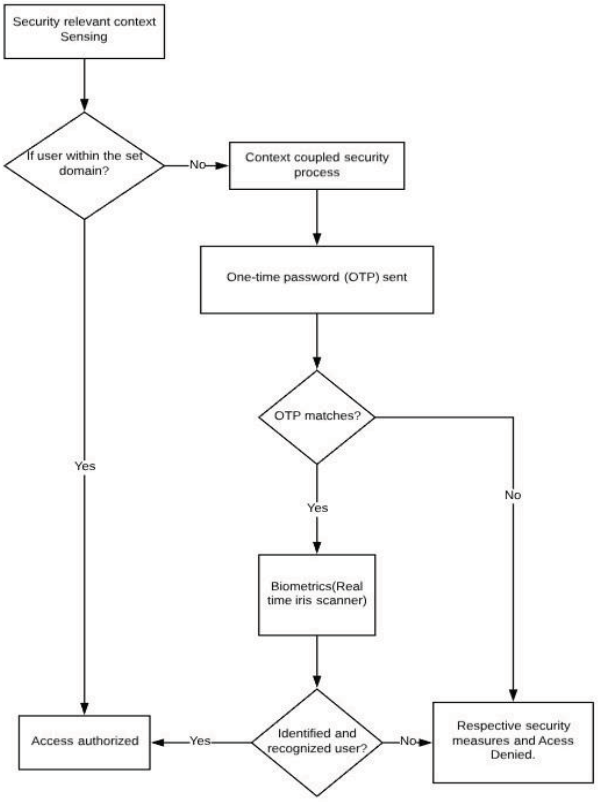

Fig. 2. Context-Aware Biometric Security Framework

This framework is proposed for security in cyber-physical system by combining contextual and real-time mechanisms. We intertwine security-pertinent setting information into different security estimates, for instance, confirmation, encryption, key understanding tradition, get the chance to control and so on. As needs be, security instrument for computerized physical structure can be capably changing in accordance with the physical condition by assistance of setting coupling. But we also provide real time security features such as OTP and biometrics (eye scan) which adds additional layers to the security realm. This multi factor authentication security mechanism is called context-aware biometric security framework. Context is the course of action of normal settings that chooses an application's lead or where an application event happens [18]. The setting can be various data providers and be vacillating shapes from temperature to survey of feelings and emotions. Context can be a remote system status, client setting area, lighting, temperature, climate, time and so on.

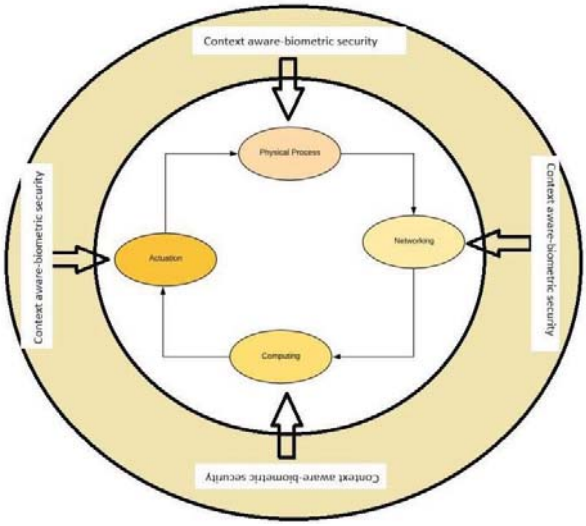

Fig. 3. Context-Aware Biometric Security Layers

In this structure, we fundamentally handle security applicable setting which comprises of the arrangement of logical properties, which is the main layer of security. Further we provide flexibility to the system without compromising the security by providing OTP for out of context authorization coupled with biometric for granting access. Therefore a person out of context (say his working environment) wants to access data, instead of denying access by identifying context mismatch as threat, we can give provisions for OTP and eye scan which enables authorization. Access is denied if any of the two factor authentication fails. In the biometric security for CPS, we consider 3 main aspects: sensing security, cyber security, control security.

A. Sensing security

We must ensure that context information is trustworthy if security configuration depends on context. We can make utilization of Trusted Platform Module to accomplish the objective of secure distinguishing. A Trusted Platform Module (TPM) [19] is relatively cheap gear used to energize building in programming frameworks. On a basic level, the sensor center point stage will involve ARM11 chip [20], outer memory, Flash and SDRAM, a transmitter, temperature sensor and battery worked control supply.

B. Cyber Security

It incorporates communication security and also security related to computation. To secure both inter and intra communications of the Cyber-Physical System from adversaries such as we have seen before, we can implement context-incorporated communication protocols.

C. Control Security

These security arrangements fundamentally center around information security just, yet their impacts on estimation and control calculations must be examined for giving inside-out safeguard against different assaults on CPS. These security measures ensure context aware security features to which OTP and biometric technology can be added.

VII.CONCLUSION

This manuscript scrutinizes the cyber security challenges and network the problems of CPS and introduced a security background for CPS along with biometrics. The goal of this paper is to confer technical knowledge within the readers mind and to substantiate the problems of cyber-physical systems.

REFERENCES

[1] E. K. Wang, Y. Ye, X. Xu, M.Yiu, L.C.K.Hui, K.P.Chow, " Issues and Challenges for Cyber Physical System", 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing.

[2] K. Wan, K.L. Man, D. Hughes, "Specification, Analyzing Challenges and Approaches for Cyber-Physical Systems (CPS)", Engineering Letters,issue3, EL_18_3_14, 2010.

[3] E. Mills, "Hackers broke into FAA air traffic control system", The Wall Street Journal, page A6, 2009.

[4] L. Neal, "Researchers Fight to Keep Implanted Medical Devices Safe from Hackers", Computer, Volume 43, Issue 8, Pages: 11-14, August 2010.

[5] K. O'Connell, "CIA Report: Cyber Extortionists Attacked Foreign Power Grid, Disrupting Delivery", Internet Business Law Services, http://www.ibls.com/internet_law_news_portal_view.aspx?id=1963& s=latestnews, 2008.

[6] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson,H. Shacham, and S. Savage. "Experimental security analysis of a modern automobile", In Proceedings of the 31st IEEE Symposium on Security and Privacy, May 2010.

[7] V. Fuhrmans, "Virus Attacks Siemens Plant-Control Systems", The Wall Street Journal, july 22, 2010.

[8] J. A. Stankovic, I. Lee, A. Mok, and R. Rajkumar, "Opportunities and obligations for physical computing systems", IEEE Computer, 38(11):23–31, November 2005.

[9] J. Madden, B.McMillin, and A. Sinha, "Environmental Obfuscation of a Cyber Physical System - Vehicle Example", Workshop on 34th Annual IEEE Computer Software and Applications Conference, 2010.

[10] D. Work, A. Bayen and Q. Jacobson, "Automotive Cyber Physical Systems in the Context of Human Mobility", National Workshop on High- Confidence Automotive Cyber-Physical Systems, Troy, MI, 2008.

[11] J. Han, A. Jain, M. Luk, and A. Perrig, "Don't sweat your privacy:Using humidity to detect human presence", In Proceedings of 5th International Workshop on Privacy in UbiComp(UbiPriv'07), September 2007.

[12] N. Pham, T. Abdelzaher, S.Nath, "On Bounding Data Stream Privacy in Distributed Cyber-physical Systems", 2010 IEEE

International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2010.

[13] W. Stallings, "Cryptography and network security: principles and practice", Prentice Hall, 5nd Edition, ISBN-10: 0-13-609704- 9,2010.

[14] J. Kao and R. Marculescu, "Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006.

[15] R. Saltzman, ASharabani, "Active Man in the Middle Attacks, A Security Advisory", A whitepaper from IBM Rational Application Security Group, February 27, 2009.

[16] K. Pelechrinis , M. Iliofotou , "Denial of Service Attacks in Wireless Networks: The case of Jammers", UC Riverside Department of Computer Science and Engineering, 2006.

[17] E. Colbert, "Security of Cyber-Physical Systems",Published in Journal of Cyber Security and Information Systems,Volume: 5 Number: 1 Cyber Science & Technology at the Army Research Laboratory (ARL).

[18] F. Gui, "Development of a New Client-Server Architecture for Context Aware Mobile Computing", PHD Thesis, Florida International University, 2009.

[19] Escrypt whitepaper, "Trusted Computing Technology for embedded Systems", 2009.

[20] Y. M. Yussoff, H. Hashim, "Trusted Wireless Sensor Node Platform", In Proceedings of the World Congress on Engineering ,Vol I,WCE 2010, June 30 - July 2, London, U.K., 2010.