Handling Multifacets of Trust Management in Cyber Physical Systems

Manas Kumar Yogi

Abstract: ***Trust should be learnt from history and context sensitive. It should not be absolute in nature. Due to the conglomeration of various technologies in a secure cyber physical system it is quite a challenge to handle trust issues in a cyber physical system. Trust management in cyber physical system is needed due to increase in the degree of autonomy, decentralized policies ,dynamic environment, decision-making based on social rules,customs,laws,values, and ethics. This chapter brings light into the existing strategies already applied by few organizations, their inherent benefits and consequent shortcomings too. There are many factors contributing towards the establishment, expression, evaluation ,maintenance of trustworthiness. In this chapter we advocate a novel framework for trust management which stands up to the research directions of how to build a unified framework for trust management, how to modify the way we compute trust, how to decide the right granularity for a trust model.***

Keywords : Trust,, Policy ,Reputation, Request, Credential, Revocable.

I. INTRODUCTION

The developing many-sided quality of the artificial intelligence and the connection of autonomous areas, for example, flight, mechanical autonomy and car is a noteworthy block against a comprehensive view CPS. Moreover, expansion of correspondence systems have expanded the span of CPS from a client driven single stage to a generally circulated system, frequently associating with basic foundation, e.g., through shrewd vitality activity. Cyber Physical Systems (CPS) comprise of a mix of various installed subsystems, which work freely of one another and furthermore cooperate with the outside condition. Such implanted frameworks work within the sight of characteristic vulnerability, setting conditions and ill-disposed sureness emerging from both the cyber and physical universes. Security is one of the key ideas to shield the CPS condition and distinctive implanting gadgets with the end goal to have a dependable and secure correspondence stage. There are numerous security methodologies and strategies proposed and executed all inclusive with the end goal to anchor CPS, alongside regions, for example, social building, security measures, merchant control, and also get to control usage, and so on. Nonetheless, notwithstanding these zones, another essential idea, specifically trust, is noteworthy in guaranteeing secure and dependable correspondences in CPS. In the current best in class, none of the current methodologies talks about the issue of a protected, trust-based CPS. Along these lines, to address this weakness, in this paper, a two-level cover approach is proposed comprising of interior and outer layers of trust among various elements to make dependable and secure CPS. This trust-based structure enhances the certainty of secure substances joining the CPS framework and furthermore assembles connections among elements, along these lines expanding the security shielding the shaped CPS from outside dangers and assaults. Currently most of the trust in CPS are realized using following principles. First one is protecting critical infrastructure from malware threats by separating non-critical from critical operations and concentrating on using hardware isolation to protect control of physical systems. Secondly, Ensuring that any code that has critical operations must be auditable by operators through source code review. The third one accounts for the attestability of processing environment. During operation, each component must be able to verify that data is received and sent only from trustworthy sources. A component also needs to attest its trustworthiness to other components. The last one is minimizing number of entities that needs to be trusted. Reducing the number of trusted entities significantly reduces the attack surface for critical infrastructure. In the ideal trusted CPS solution, the operator will maintain the only root of trust for critical code execution. Social trust is extremely mind boggling and relies upon numerous variables, which makes is hard to display in a computational framework. A few variables which impact trust are: past experience with a man, association with the individual, suppositions of the activities a man has taken, psychological factors affected by a lifetime of history and occasions, talk, and influence by others' assessments. Much work has been done to formalize the idea of social trust into registering situations.

There are three principle properties of assume that are significant to creating trust-based computational models: transitivity, asymmetry, and personalization . This exploration endeavors to display every social property in the processing condition to precisely reflect the thought of social trust. The possibility of transitivity is that social trust can be passed between individuals. For instance, Alice profoundly confides in Bob, and Bob very trusts Chuck, despite the fact that Alice does not know Toss, she could in any case determine some feeling of reliability for Chuck. In any case, trust is not splendidly transitive in the numerical sense, since it would not be the situation that Alice profoundly confides in Chuck, a man she has no past connections with. There has been much research in demonstrating the transitivity of trust, additionally alluded to as trust proliferation. Scientists have built up a formal structure of trust engendering plans. Their structure accept that clients unequivocally state trust esteems in different clients. They have moreover presented the idea of doubt and the spread of doubt, which has not been done in past research.

Revised Manuscript Received on August 05, 2019.

Manas Kumar Yogi*, Asst. Prof. CSE Dept., Pragati Engineering College(A),Surampalem,A.P.,India .

They directed tests on the Epinions.com dataset, and inferred that few communicated trust proclamations for each client, permits the framework to foresee trust between any two individuals in the framework with high precision. The property of trust is critical. In the event that two individuals are engaged with a relationship, the trust which they hold for each other won't really be indistinguishable. Since people are so one of a kind in their terms of their own encounters, foundations, and accounts, it is straightforward the nature of trust. In the application to shared separating, trust varies from likeness, in that closeness is symmetric. This is an imperative contrast since trust enables clients to frame extra associations which were impractical with comparability esteems. The last property is personalization of trust. Trust is an emotional, sincere belief. Two individuals frequently have altogether different assessments about the reliability of a similar individual. Personalization assumes an imperative job in making suggestions to a client. It is the personalization of trust which enormously influences the precision of a proposal. The proposed demonstrate in this work, endeavors to register trust esteems on a fine-grained, customized level.

II. VISION FOR FUTURE FOR TRUST MANAGEMENT

2.1 Decision Support based on Trust Management

The secure CPS should be able to take decisions based on recommendations given by the trust management framework. A trust-aware recommendation architecture should be made which should depend on users directly mention trust values for other CPS entities. They could also use a robust trust propagation mechanism which can be applied to the network of users, to determine a trust weight that can act as a substitution for the similarity weight. Such type of systems can lower the average error on predictive accuracy for cold start users.

2.2 .State of Nature: Are the (other) CPS systems trustworthy? The idea is to develop a trust model which uses quantitative and qualitative factors to construct trust relationships between entities based on their common choices. Trust propagation principle can be applied to lengthen the trust relationships beyond the direct neighbors. A trust framework can make a record of hops for trust propagation. If hops are more along a system of secure CPS, then it represents a more trustworthy path.

2.3 Certifications by trusted authorities: Vendors who have a stake in a CPS system should develop a certification standard for participating entities which instills confidence, trust among the network entities.

2.4 Loss Function: It has to be suitable defined. In case of malicious attacks for a CPS, a measure has to be developed to gauge the extent of trust lost. This measure should be accurate enough to help the concerned persons to initiate procedures to safeguard the remaining trust values in the system .It is one of the most difficult research challenges.

III. TRUST PROPAGATION STRATEGY IN SECURE CPS

All clients in the area turn into the arrangement of direct neighbors, D, for target client. Each immediate neighbor, d I , will proliferate their trust esteems to their best m most reliable neighbors .The spread trust esteems will be put away and utilized amid the forecast procedure. These clients turn into the optional neighbors in the trust-arrange for the objective client. When the trust-arrange is framed, the rating forecast is created. The main distinction is that the optional neighbors utilize the engendered trust esteems as information.

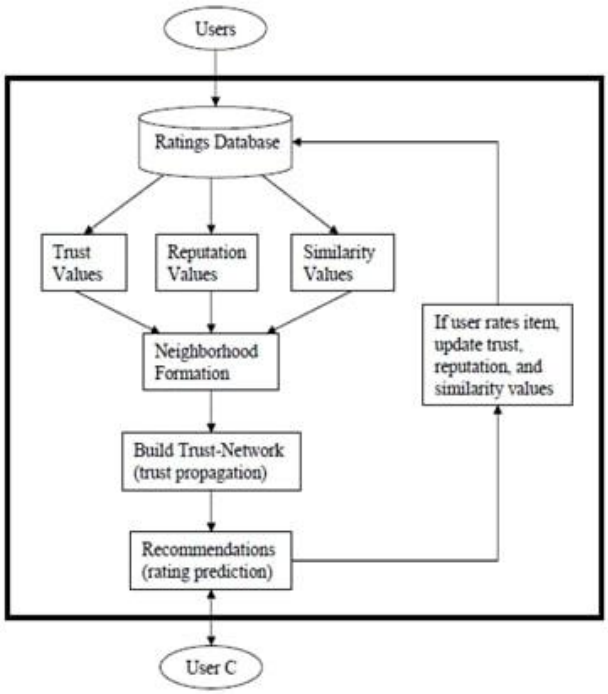

Fig.1.Proposed technique

Figure 1, gives an outline of the Trust Propagation technique. Trust, notoriety and similitude esteems are figured from the chronicled appraisals information. These qualities are utilized to fabricate an area for the objective client. The individuals in the area turn into the immediate neighbors, who at that point spread their trust esteems to different individuals in the network. This structures a trust-organize for the objective client, or, in other words produce rating forecasts and distinguish recommendable things.

Customary cooperative sifting utilizes the k-Nearest-Neighbors way to deal with distinguish the suggestion accomplices. This strategy recognizes the best k clients dependent on the comparability, trust, and additionally notoriety esteems. These best k clients frame the area for the objective client. These neighbors are then used to produce rating forecasts. A second way to deal with neighborhood development is to distinguish the objective thing first, and afterward frame the area dependent on the specific thing. The objective thing is the thing we have to create a forecast for. The thought is to sift through all clients who have not evaluated the objective thing. On the off chance that a client has not appraised the objective thing, they are avoided from partaking in the expectation procedure. This area arrangement strategy is called k-Nearest-Recommenders (kNR) . The initial step is to inquiry the client database to recognize all clients who have evaluated the objective thing, and afterward the best k neighbors are picked dependent on the comparability, trust, as well as notoriety values. The kNR strategy will just consider clients who have the expected data to make a forecast. This varies extraordinarily from the k-Nearest-Neighbor approach, where the objective client's neighborhood stays static.

The kNR technique requires more computational overhead, since it powerfully constructs another area for the objective client for each evaluating expectation. The advantage to kNR, is that once the area is shaped, it is ensured that a rating forecast can be produced. Interestingly, an area worked with the kNN approach, should initially guarantee that something like one neighbor has appraised the objective thing, and at exactly that point can a rating forecast be produced. Both neighborhood development techniques will be actualized and tried amid the assessment of the trust-based suggestion procedures.

The steadfastness and cyber security prerequisites that shape the reliability stage utilize a blend of lower level necessities generally present in physical handling and PC organize frameworks. Framework operational accessibility, unwavering quality, viability, and security prerequisites are very much concentrated in the assembling writing and are not the subject of this work. On the digital world side, the cyber security necessities are a piece of the PC and system security areas, however have not been concentrated in detail from the assembling condition point of view. The genuine prerequisites recorded in Fig. 1 is likely precedents of what trustworthiness and cyber security prerequisites would be for genuine appropriated producing tasks. Accessibility, unwavering quality, and practicality of assembling gear is characterized by its sellers, so it could change dependent on the extension and assets. Wellbeing prerequisite is standard for programmable controllers in the process control industry, be that as it may, by and by, it could shift dependent on the degree and asset. Secrecy, honesty, and information accessibility are known in the security network . Secrecy guarantees security of information from divulgence to unapproved parties and is normally upheld through information encryption. Trustworthiness guarantees information insurance from being changed by unapproved parties and is typically guaranteed through documenting and excess of information transmission. Accessibility guarantees that approved gatherings can get to the information when required, and it is acquired through various instruments that shield the framework and information from outer assaults, for example, forswearing of administration assaults. The other two cyber security prerequisites, realness and confirmation are reciprocal and further help circulated producing on-screen characters in reliable information exchanges through advanced mark abilities and authorization and security instruments.

An exponential development in the improvement and sending of different kinds of cyber-physical systems (CPSs). They have brought effects to all parts of our day by day life, for example, in electrical power grids, oil and gaseous petrol dissemination, transportation systems, human services gadgets, family apparatuses, and some more. A significant number of such systems are sent in the basic foundation (CI), life bolster gadgets, or are fundamental to our everyday lives. Along these lines, they are required to be free of vulnerabilities and resistant to a wide range of assaults, which, sadly, is essentially outlandish for all genuine systems.

One crucial issue in CPS security is the heterogeneity of the building squares. CPS are made out of different components from multiple points of view. There are diverse equipment components, for example, sensors, actuators, and inserted systems. There are likewise extraordinary accumulations of programming items, restrictive and business, for control and observing. Accordingly, every segment, and in addition their coordination, can be a contributing component to a CPS assault. Understanding the present CPS security vulnerabilities, assaults and insurance instruments will give us a superior comprehension of the security stance of CPS. Therefore, we ought to be capable bring up the restrictions of CPS that make them subject to various assaults and devise ways to deal with safeguard against such assaults.

The multifaceted nature of CPSs and the heterogeneity of CPS segments have acquainted critical challenges with security and protection assurance of CPS. Specifically, with the complex cyber-physical associations, dangers and vulnerabilities wind up hard to evaluate, and new security issues emerge. It is likewise hard to distinguish, follow, and look at the assaults, which may begin from, move between, and focus at various CPS segments. A top to bottom comprehension of the vulnerabilities, dangers, and assaults is fundamental to the improvement of barrier instruments. A study of existing CPS security and protection controls will likewise empower us to distinguish missing pieces, feeble connections, and new investigations.

To start with, identifying how CPS is different from legacy control systems or traditional IT systems is one of the major and primary things that everyone should know which in-turn lead to study of security problems that are being faced in the Cyber Physical Systems. The privacy and security in the cyber physical system can be observed using the framework with three perspectives which are CPS components, CPS systems and Security. In terms of security as first perspective, threats, attacks and vulnerabilities and controls are highlighted. For the next perspective of Cyber Physical System Components: it is cyber, physical, and cyber-physical components. Speaking cyber physical system components as attacks, they can be categorized as cyber-attacks, physical attacks and cyber-physical attacks. Final perspective of Cyber physical Systems models like smart grid, smart cars, medical device and Industrial Control systems (ICS).

There is no universally accepted definition for cyber physical systems however, a statement that can define is cyber physical systems are generally the systems that alters, authorize and govern the physical world of networking systems with the advancement in the technology. This led cyber physical systems to involve with embedded systems using actuator and sensors kind of things together integrated and form various models of cyber physical systems. As dependency of IT systems in CPS, integration of information and communication technologies (ICTs) to enhance interactions with physical processes. This led to various physical world application systems in our daily life in various fields like energy, transportation, military, healthcare, and manufacturing. Depending on the situation, purpose and fulfilment of the need the cyber physical system model and name of the application model changes.

Rather than security problems, the issue that Cyber Physical Systems that are going to face is data analysis. As the systems are widely distributed across the globe, extensive amount of data has been emerged where decision making and data analysis on information that was gathered became a hurdle task.

To process the data different technologies are various learning algorithms has to be proposed. Data collection is itself not simple step that is to be performed. It is actually followed by data collection, data transmission and then data storage. This is the stages of process that is done with the data collections from distributed cyber physical systems.

Firstly, discussing about cyber physical system models that are existing currently are Smart Grids, smart Cars, medical devices and Industrial Control Systems.

To discuss about disparate collection of cyber physical systems, it involves complexity and integrity of the systems. A smart grid with an immense deployment of home energy management system and advanced metering infrastructure has been developed which is a transformative shift of classical grid that is more reliable and secure. A well-known example for the smart grid security is power grid where the structure is a complex cyber physical system that support the need of human as there is increase in the population to satisfy their daily needs appliances to regulate the power supply.

Industrial Control Systems:

ICS alludes to control systems used to upgrade the control, observing, and generation in various ventures, for example, the atomic plants, water and sewage systems, and water system systems. Here and there ICS is called SCADA or disseminated control systems. For consistency, we will utilize the term ICS henceforth. In ICS, diverse controllers with various capacities work together to accomplish various expected objectives. A well known controller is the programmable rationale controller (PLC), or, in other words intended to work persistently in antagonistic conditions. This field gadget is associated with the physical world through sensors and actuators. As a rule, it is furnished with remote and wired correspondence limit that is designed relying upon the encompassing situations. It can likewise be associated with PC systems in a control focus that screens and controls the activities.

communication achieved: Two classifications of correspondence conventions are sent in ICS, one is utilized for the computerization and control, for example, Modbus, Distributed Network Protocol (DNP3), and the other is for interconnecting ICS control focuses, for example, Inter-Control Center Protocol (ICCP).

Smart Grid:

The smart grid is imagined as the up and coming age of the power grid that has been utilized for quite a long time for power age, transmission, and appropriation. The smart grid gives a few advantages and propelled functionalities. At the national level, it gives upgraded emanation control, worldwide load adjusting, smart age, and vitality investment funds. Though at the neighborhood level, it permits home buyers better power over their vitality utilize that would be gainful financially and earth.

The smart grid consists of two major components:

1) power application and

2) supporting infrastructure.

The power application is the place the center elements of the smart grid are given, i.e., power age, transmission, and conveyance. Though the supporting framework is the wise part that is primarily worried about controlling and observing the center activities of the smart grid utilizing an arrangement of software, hardware equipment, and correspondence systems.

Communication achieved: The networks are of two kinds: field gadget interchanges inside substations utilizing Modbus and DNP3, and as of late the further developed convention, created by the International Electrotechnical Commission (IEC), IEC 61850. The other sort is control focus interchanges, which additionally depend on ICCP, like ICS. Moreover, smart meters and field gadgets utilize remote interchanges to send estimations and get directions from control focuses. Smart meters, for instance, utilize short-extend recurrence signals, e.g., ZigBee, for diagnostics tasks by professionals or readings by advanced smart peruses.

Medical Devices: medical gadgets have been enhanced by incorporating cyber and physical capacities to convey better medicinal services administrations. We are more intrigued by therapeutic gadgets with cyber capacities that have physical effect on patients. Such gadgets are either embedded inside the patient's body, called IMDs, or worn by patients, called wearable gadgets. They are typically outfitted with remote capacities to permit correspondence with different gadgets, for example, the software engineer, or, in other words refreshing and reconfiguring the gadgets. Wearable gadgets speak with one another or with different gadgets, for example, a remote doctor or smartphone.

Communication achieved: It is an important prerequisite that IMDs be designed and refreshed remotely, with the goal that no careful extraction for the gadget is required. Hence, remote correspondence is the most widely recognized technique for correspondence in therapeutic gadgets. IMDs and wearable gadgets depend on various correspondence conventions and advancements. For instance, IMDs utilize low recurrence (LF) signals indicated by the Federal Communications Commission, called Medical Implant Communication Service, that make it workable for IMDs and their software engineers to convey. Then again, wearable gadgets depend on another sort of remote interchanges, i.e., body zone organize (BAN). Boycott uses a few remote correspondence innovations, for example, Bluetooth and ZigBee.

Smart Cars:

Smart cars (canny cars) will be cars that are greater condition benevolent, eco-friendly, safe, and have upgraded amusement and comfort highlights. These headways are made conceivable by the dependence on a scope of 50– 70 PCs arranged together, called electronic control units (ECUs). ECUs are in charge of checking and controlling different capacities, for example, motor discharge control, brake control, amusement (radio and mixed media players) and solace highlights (journey control and windows opening and shutting).

Communication achieved: Smart cars can have diverse kinds of correspondence limits, including vehicle to vehicle (V2V), vehicle to foundation (V2I), and in-vehicle interchanges. In this paper, we center around the last mentioned. As we made reference to, cars have around 70 associated ECUs, all of which impart through a transport arrange. The system is generally partitioned into different subnetworks, every one of which likewise has a transport topology. Subnetworks can trade messages through a portal that isolates their traffics. A typical origination is that this partition is because of security concerns.

The mostly used protocols here

1) The local interconnect network (LIN), utilized for generally low speed applications, for example, opening/shutting windows.

2) Controller area network (CAN), utilized for delicate constant applications, for example, the electronically monitored slowing mechanism (ABS).

3) Flexray, required for hard ongoing applications where the speed of transmission is basic, for example, braking or reacting to a snag before the car.

4) Media oriented systems transport, utilized for in-car entertainment applications .

IV. CONCLUSION

This paper advocates a structure for the advancement of reliability answers for assembling cyber physical frameworks, which incorporate steadfastness and cyber security prerequisites. Point by point demonstrating is performed for the cyber security perspectives by displaying a progression of dissent of administration assaults against a general assembling system shaped by physical and cyber world hubs. The after effects of the re-enactment ponder demonstrate that the cyber strength systems are better conveyed when the quantity of system hubs is bigger to allow re-steering of bundles in the system. By summing up the outcomes, it might be conceivable to adjust the answer for the cyber versatility of arrangement of-frameworks models, in which case it might end up obvious that the strength of the arrangement of-frameworks level is higher than that of individual part frameworks of the arrangement of-frameworks. Future research headings incorporate the investigation of other cyber security assaults and their impact on the segment level and framework level cyber flexibility. On another heading, the work can be upgraded by adding different dependability parts to the framework flexibility show and assess their effect on the inferred strength measurements.

REFERENCES

1. R.F. Babiceanu, R. Seker, Big data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook, Computers in Industry, 81 (2016) 128-137.
2. R.F. Babiceanu, R. Seker, Manufacturing operations, Internet of things, and big data: Towards predictive manufacturing systems, in: T. Borangiu, D. Trentesaux, A. Thomas, (Eds.), Service Orientation in Holonic and Multi-Agent Manufacturing, Springer Studies in Computational Intelligence, 594 (2015), pp. 157-164.
3. R.F. Babiceanu, R. Seker, Manufacturing cyber-physical systems enabled by complex event processing and big data environments: A framework for development, in: T. Borangiu, D. Trentesaux, A. Thomas, (Eds.), Service Orientation in Holonic and Multi-Agent Manufacturing, Springer Studies in Computational Intelligence, 594 (2015), pp. 165-173.
4. M. Goodman, Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About It, Random House, New York,2015.
5. P.A.A. Ralston, J.H. Graham, J.L. Hieb, Cyber security risk assessment for SCADA and DCS networks, ISA Transactions, 46 (2007) 583-594.
6. L. Wang, M. Torngren, M. Onori, Current status and advancement of cyber-physical systems in manufacturing, Journal of Manufacturing Systems, 37 (2015) 517-527.
7. L.J. Wells, J.A. Camelio, C.B. Williams, J. White, Cyber-physical security challenges in manufacturing systems, Manufacturing Letters, 2(2014) 74-77.

AUTHORS PROFILE

Mr. Manas Kumar Yogi pursued Bachelor of Technology from VR Siddhartha Engineering College,Vijayawada,A.P. in 2006 and Master of Technology From Malla Reddy College Of Engineering And Technology in year 2012. He is currently working as Assistant Professor in Department of Computer Science Engineering , Pragati Engineering College (Autonomous), Surampalem, East Godavari District, since 2014. He is a member of IEEE & ACM since 2014. He has published more than 80 review,research papers in reputed international journals ,conferences including IETE sponsered conferences. His main research work focuses on Software Engineering, Distributed Computing, Cloud Security and Privacy, Big Data Analytics, , IoT and Computational Intelligence based optimisations. He has 9 years of teaching experience and 2 years of software industry Experience.