Devising a Secure Architecture of Internet of Everything (IoE) to Avoid the Data Exploitation in Cross Culture Communications

Asim Majeed
School of Computing and Digital Technology
Birmingham City University (BCU)

Anwar Ul Haq
Department of Computer Science
QA Higher Education (ULST)

Rehan Bhana
School of Computing and Digital Technology
Birmingham City University (BCU)

Mike-Lloyd Williams
Department of Business Administration
QA Higher Education (ULST)

***Abstract*—The communication infrastructure among various interconnected devices has revolutionized the process of collecting and sharing information. This evolutionary paradigm of collecting, storing and analyzing data streams is called the Internet of Everything (IoE). The information exchange through IoE is fast and accurate but leaves security issues. The emergence of IoE has seen a drift from a single novel technology to several technological developments. Managing various technologies under one infrastructure is complex especially when a network is openly allowing nodes to access it. Access transition of infrastructures from closed networked environments to the public internets has raised security issues. The consistent growth in IoE technology is recognized as a bridge between physical, virtual and cross-cultural worlds. Modern enterprises are becoming reliant on interconnected wireless intelligent devices and this has put billions of user's data in risk. The interference and intrusion in any infrastructure have opened the door of public safety concerns because this interception could compromise the user's personal data as well as personal privacy. This research aims to adopt a holistic approach to devising a secure IoE architecture for cross-culture communication organizations, with attention paid to the various technological wearable devices, their security policies, communication protocols, data format and data encryption features to avoid the data exploitation. A systems methodology will be adopted with a view to developing a secure IoE model which provides for a generic implementation after analyzing the critical security features to minimize the risk of data exploitations. This would combine the ability of IoE to connect, communicate, and remotely manage an incalculable number of networked, automated devices with the security properties of authentication, availability, integrity and confidentiality on a configurable basis. This will help clarify issues currently present and narrow down security threats planning considerably.**

Keywords—privacy; privacy enhancing technology (PET); big data; information communication technology (ICT)

I. Introduction

The Internet of Everything (IoE) can be defined as the products and systems which are communicating and interacting with the environment, users and another system through the communication networks. The emergence of IoE has integrated various diverse type networks and wireless communication technologies under one platform [3]. The new open communication relationship among devices has complicated the trust relationship and raised security issues within communication systems and the heterogeneous entities. The IoE based organizations require a novel security architecture to be laid out after analysing the existing ICT infrastructure to solve these security issues [5]. The IoE among cross-cultural organisations is growing at an alarming pace and meeting the security demands is becoming hyper-complex since the advancement in capabilities of smart technologies. The cross-cultural communication creates vulnerabilities and cyber security challenges depending on the communication processes, products and security of data; consequently have a high impact on economic growth [19]. The integration of various devices on a multichannel enhances users experience but positions the organisation's interface where intruders could exploit the data. Organisations operating in various sectors of the world have potentially many business partners, advisers, customers and closer collaborations exchanging a significant amount of data with each other. This not only enriches the product development and recruiting experience but leaves information's flaws in complex data handling. Cross-cultural organisations using hybrid delivery models run processes and business services through the cloud; managed by external providers [10]. The hybrid models help organisations to look at the activities through IoE communication model and extend the security perimeter to detect and monitor cyber security attacks.

Cross-cultural awareness and understanding are becoming increasingly important in the modern era. The study conducted by Botha et al, [3] showed that young people are particularly comfortable in sharing their experiences and cultural signatures through mobile technology and SMS services. Smartphones were at the forefront of the technology from the late nineties until now. Increasingly smart devices and wearable technologies are driving a new technological revolution [18]. These devices are capable of using sensor technologies to monitor, alert, automate the processes and activities in our personal and work lives. The world is increasingly becoming more global and the advent of new digital technologies is constantly diminishing the barriers of space and distance among communities. At a global scale, this phenomenon is presenting new challenges in terms of how to increase the awareness of the cultural sensitivities and safe-use in the new digital era of Internet of Everything (IoE) [12].

The evolution of computers from mainframes to PCs, the transformation into ubiquitous computing with the emergence of Wireless sensor networks lead to wide industry adoption of Internet of Everything [13]. Due to this rapid evolution process, Internet of Everything has become an integral part of our life in the form of smart homes, smart healthcare, and smart automobiles [17]. Similarly, this advancement in technology is becoming de facto standard for businesses to achieve their key performance indicators and remain on the cutting edge in this competitive market [13]. Although currently customer-centric approach is helping businesses to create positive customer experiences with the help of analytic techniques, which analyses Big Data and can add value to a company, a more intelligent approach is required to deal with real data involved in Internet of Everything [15]. It is expected that the number using the Internet of Everything, will grow up to 50billion by 2020. This is due to the fact that transitioning to Internet of Everything by adding intelligence to data, allowing continuous monitoring, updating and controlling it in a real time improves the operational decision-making process of business [8].

II. 'IOT-IZING' THE BUSINESS

The adoption of latest technologies is slow particularly in small businesses but IoE integration has envisaged all size businesses to add real value to their communications and day to day processes [2]. Modern businesses are required to be proactive to build a frame around of how they can stay IoT-ized especially in meeting the cross-cultural communication needs. As soon as an organization starts thinking about moving their internal and external communications and processes on IoE related technologies, they would need to think investments on resulting data, volume of data connectivity, infrastructure support, data intelligence and sensors [20]. Consequently, businesses would need to think about staff training of using the IoE technologies to take the full advantage of going IoT-ized [18]. The integration of IoE technology based infrastructure would also help cross culture staff training to stay up to date on the updates and changes taking places within the organizations. The journey of going IoT-ized would bring unexpected and unpredictable challenges in real time situations but cross culture conflicts and consortiums could be resolved to share best practices using IoE paradigm [12]. The management of cross-culture communications using IoE technologies to connect more and more devices would bring more opportunities for cyber criminals as well as hackers [6].

It is very important for all size businesses to consider the security threats to avoid risks of data exploitation. If businesses are using some devices for communication and recording, there is a huge risk of these devices can be hacked and information recorded in this device could be exploited [5]. These threats should be embraced as a challenge to the organization and design a framework which could authenticate and authorize the secure users only and if the infrastructure triggers any caution about a unauthenticated device, the access should not be allowed. Capgemini's, [4] survey shows the Internet of Everything (IoE) present a business opportunity for a trillion-dollar industry and growth of new industries to cater for this shift where technology infused the world is a norm. The 71% of executives (related to IoE industry) raise their concern on security threats and related consequences on the growth of this business and opportunity it presents [4]. Only 33% of executives in the survey believed that the current IoE based products and services are resilient to cyber security attacks [4]. One of the key factors for the increase in security threat is the fact that IoE based products and system increase the potential attack points in a system [5]. The users awareness and patterns of behavior could play a major role in safe-use of IoE based products and systems [18]. The understanding of cultural behavior and patterns of communities will also play a key part in the growth of IoE based industry, especially when a culture of one community may affect the culture and behavior pattern of another community in terms of educating and informing the safe use of IoE based products and systems [1].

Fig. 1. IoT-izing and Cross Culture Communication [4]

The adoption of Internet of Everything provides business data intuitiveness, which was never possible before [12]. Increased processing power of server machines, super-fast internet connection, and massive use of smart devices with their falling costs, seamless business to business communication and development of applications lead the businesses to adopt cloud-based solutions, to help achieve scalable, flexible and low-cost solutions to improve their customer experience [3]. Just establishing IT infrastructure and connecting to The Internet is not enough, the adoption of IoE and cloud services is also required for a business to improve its informed decisions by the stakeholders [2]. Cloud services allow storing and analyses of business data coming from different streams [4]. Internet of Everything will constantly generate new data, which can be used to enhance the business key performance indicators such as customer services [6]. In order to gain an advantage of the Internet of Everything, companies should proactively plan to which extent they can be 'IoT-ized ' [3]. This can be done by focusing on the installation of infrastructure and employee training, so they can handle both internal processes and customer's queries [9]. Internet of

Everything is all about the connection between devices and exchanging of data, which means there are increased security threats to data and devices [5]. As more and more new devices are connected to IoE, people must be made aware of how to implement security measures while connecting these devices; they also provide new opportunities to the hackers because the experts are also exposing more vulnerabilities [4].

A. Privacy in IoE

Since the IoE has become so widespread, the smart devices know more and more about how to collect our data, therefore, we should also be aware of how they are monitoring and collecting our data and spying on us without our consent [8]. Security and privacy are one of the critical concerns individuals have. The EU Commission's paper on Internet of Everything Governance also highlights the implementation of security controls to minimize cyber-attacks and individual surveillance [14]. This does not mean that Internet of Everything should be avoided but rather a cautious and planned approach should be taken [2]. The dawn of internet has raised the concerns over privacy preservation. When organizations are communicating cross-culturally through the IoE medium, many applications used by the devices will exacerbate the problem of leaving trails of communication, traceable signatures, locations and the individual's behaviors [6].

The privacy concerns of healthcare organizations are more relevant as they run many applications through IoE. The hospital management systems may require the tracking of medical equipment or the monitoring of patient's vital statistics within assisted living facilities or at home. In this situation, the new IoE devices which require association and decoupling with the owner should authenticate the security check so to identify the device. A mechanism of shadowing has been proposed to look at the data security [8]. The user objects use digital shadows which store the virtual identity of the device in terms of its attributes and information [19]. The association of diverse authentication methods for machines and humans would offer new opportunities to identify the device identity and increase security. The door of personal networks could be opened for an object combining it with bio-identification [20]. Different countries have different views on compliance and privacy especially since technology is consistently evolving on a daily basis and cross culture organizations need to be cognizant of how these matters and issue would apply to them [11].

III. Cross Culture Communication and IoE

In order to meet the current demands, businesses are advancing their technologies in both software as well as hardware. Various researchers and IT experts have warned that this model is going to be changed in the future especially in terms of IoE advances when looking at cross-cultural aspects. This model would lead to the concept of generating revenue not only from hardware but from its use of on a cross culture communication basis. The model of freemium subscriptions would be the preferred choice in the IoE era of cross culture organizations [9]. The assumed model would raise many security issues relating to user's data. The services designed around hardware would be more amenable to ecosystems and easily upgradable providing multiple opportunities to generate revenue [14]. The evolution of a service-centric model could result in cross culture businesses struggling to ensure that they prioritize processes in order that protecting user data is easy as well as secure and transparent. Organizations would benefit from this customer-centric communication in terms of keeping track of customer loyalty program information, payment methods and purchase history [7]. This information would help organizations to improve customer experience as well as creating a solid foundation for monetization and data security [16].

IV. Elements of a Secure Architecture: Cross Cultural Business Perspective

The basic principal and central approach of IT security should be to design a secure infrastructure instead having additional layers of the existing architecture [20]. In relation to design a secure IT infrastructure for cross-culture communication, following principals need to consider:

A. Alignment of Business Domains and Security Requirements

A traditional IT infrastructure is designed in alliance with business processes and domains. In particular, if we talk about the retail businesses their domain may be based on the entire value chain from store management to supply chain management [10]. On the contrary, the IT infrastructure design has to look at both the perspectives of risk exposures to existing assets and business processes in each domain. The security element should be embedded and made an integral part of the architecture rather than making it more complex after adding more security layers [7].

B. Grouping by Capability

The ICT infrastructure is made secure and manageable on the basis of similar privileges level for users [2]. The privileges are assigned to particular groups of security and business domains. The risk is assessed on processes and assets of the organisations through the capability level and if it requires, more consistent and adequate securities these are assigned to various groups [11]. The homogenous level of protection is obtained after adding capabilities to security domains

C. Modularity

The modularity part deals with adjusting the security level of domains without affecting the other domains [9]. The business encompasses various domains with different security levels and modular structure as this helps to adequately measure the risk and at the same time provides protection as well. The infrastructure security could be increased by deploying the pivotal points at various nodes to monitor the technology. Devising a secure interface only between a corporate network and public internet is insufficient [18]. The threats of hijacking the network after connecting and penetrating in the infrastructure would grow. These threats would not be protected by the outside network guards and require some inside topologies to be devised to keep it secure through triggers [13]. As soon as some users get connected with the IoE, an extra security layer should be activated which detects attacks. The system should be designed in an intelligent way, which consistently observes the inside activities, detects user behavior change and alerts the infrastructure. Once the network is divided into security domains, it brings multiple benefits to detecting threats [4]

Information is a valuable source and most modern businesses rely on effective use of information for their processes, market reach, customer satisfaction and competitive advantage [9]. This demand for the valuable information puts a strain on privacy and data related to personal liking, disliking, and behaviour. Etc. The information system has brought huge success to businesses in achieving their goals. The information system gathers process, distribute, utilise and interact with information [6]. The success of information systems is dependent on channelling communications effectively between different components of such system including people. The information security is an established discipline and with well-defined procedures and measures to this effect.

V. Existing Architecture Limits

Time and the budget have always been a pressure on modern organizations even though they are willing to invest heavily to secure their IT infrastructure [8]. These constraints lead them not to integrate security triggers inside the infrastructure but layering a new security infrastructure on top of their existing IT architecture. This addition creates ring-fenced, haphazard and heterogeneous architectural landscape which requires vast system updates and manual intervention to maintain it [15]. The purpose is to develop a secure architectural infrastructure but instead, this approach creates unanticipated gaps as well as complexity in a cross culture communication environment. There will be challenges if organizations roll out automated and digitized services quickly [10]. The coding of planned pilots through the cloud should have been monitored before the launch and along the appropriate consideration of the existing landscape. The safe testing area should have been created otherwise organization would end up risking their IT infrastructure [9].

VI. A Journey Towards Devising a Secure IoE Architecture

The capabilities of secure enterprise architecture are identified through an initial security assessment and classified by threat level [1]. The most critical business assets such as underwriting data and trading algorithms are analyzed to identify security gaps. The compromise on the security gaps could lead to reputational harm as well as material losses. The processes and assets of high-risk and high-value nature are separated on the basis of threat based classifications but cross-culture communications still benefit through virtual environments and shared infrastructure [19]. Various applications and servers could be used to run the organizational website through a separate authorization engine to process the high-value financial transactions within the cross-culture communications. The activities to support process and data steps for online money transfer or other business transactions are classified under discrete capabilities [7]. The adequate level of risk and protection could be determined through the analysis of security zone architecture within the cross culture communication. The risk impact of breaching can be estimated through the regulatory, competitive, financial, reputational and operational processes of the organization [3]. The risk can also be estimated through the process downtime as this mishandling of customers personal information could lead to regulatory fines [4].

VII. Model of Secure Architecture for Cross Culture Communication: : Technical Perspective

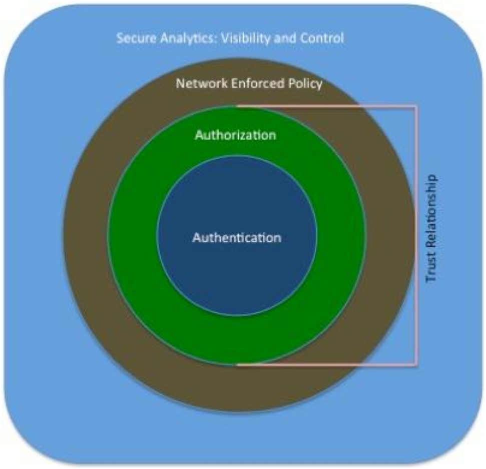

Fig. 2. Secure IoT Framework [20]

A. Authentication

The authentication layer is the central part of this framework which could be used to identify and verify the IoE entity information. As soon as the IoE devices start establishing the connection to each other, they require getting connected to IoE infrastructure [2]. The identity of the device should determine the trust relationship. Various IoE devices may have substantially different ways of storing, managing and presenting the information. It is noted that eligible users in organizations access the network for both local and cross culture communication through human credentials of password and username [4]. In terms of IoE the endpoints should be setup through fingerprint means, so not to require human interaction. The embedded sensors within the IoE devices should set artificially intelligent to scan and then recognize the user identity based on the particular device storage mechanism [12]. The X.509 certificates could also be used to establish a strong authentication system to establish this identity. The X.509 certificates are cryptographic and require enough memory to be executed consequently it may not be possible for various IoE devices to validate these certificates. The authentication protocol 802.1X defined by IEEE could also be used to authenticate the footprints leveraging the capacity to store strong human credentials and managing CPU load. The new modalities and form factors bring out the challenges of coining smaller footprint credential types based on less intensive constructs of cryptographic as authentication layer for cross-cultural communication [17].

B. Authorization

Authorization is the second layer of this framework controls all device access throughout the infrastructure environment [9]. The core authentication layer is also embedded in this by integrating the entities identity information. The exchange of appropriate information starts as soon as a trust relationship is established between authorization and authentication components [11]. The same car vendor can develop a trust alliance between his all cars, so one car can share certain safety capabilities related information with another car. This established trusted alliance relationship between cars and their dealers may allow transmitting and exchanging additional information such as their last maintenance records or odometer reading [17]. The mechanism of user's access and management to enterprise networks is well validated in the current policy structure of IoE devices. Building an architecture handling communication of billions of IoE devices with varying trust relationships would be a big challenge for cross-culture communications [18]. These challenges would also extend to the point of end-to-end communication with appropriate controls and traffic policies to segment and synchronize the data traffic. The major factor to be looked after in this architecture would be the minimization of data exploitation.

C. Network Enforced Policy

The network enforced policy layer involves the traffic of all things that will route and transport on the infrastructure securely including controlling and management of the data exchange over IoE devices. Various mechanisms and protocols are already established regarding network enforced policy to secure the infrastructure of a network when IoE devices communicate cross-culturally [20].

D. Secure Analytics: Visibility and Control

The process of controlling the IoE ecosystem with the purpose of gaining visibility, a service is defined by the secure analytics layer through which data centers, network infrastructures, and all endpoints participate in providing telemetry [15]. A massive parallel database (MPD) platform can be deployed as it would process large volumes of data efficiently [20]. The anomalies of the secured data can be picked out and real time statistical analysis could be performed when integrating analytics with this technology [4]. This is a telemetry provision of all those elements that correlate and aggregate the information required for threat detection. This model envisages that, if the data is accessed by unauthenticated and unauthorized IoE devices, threat mitigation should automatically shut down the attacker and raise those triggers. The IoE devices generate data and that is only valuable if the correct security process and analytical algorithms are applied to identify and resolve the threats [6]. The security algorithms are applied on various layers of this model and data collected from those sources could produce a better analytical outcome of dealing with security threats. Every day new technology is evolving and network fabrics are becoming more complex in nature. The infrastructures topologies are moving to private and public clouds and this move require defense capabilities along with threat intelligence detection and resolution at the same time on clouds. The derivation of accurate intelligence requires control, context, and visibility [13].

VIII. Conclusion

The IoE constructs have vast security implications so deconstructing an existing security framework could be a foundation of security for future cross-culture communications environments. The proposed framework by the authors could be used in operational environments where policy enforcement is a key feature as well as protocol lead product development frameworks. There is a huge potential for zero-day attacks since the IoE industry is consistently emerging from multi-culture communications to cross-culture communications. This offers the devised architecture to apply security at the appropriate layer. The last layer of this architecture is the end point highly constrained devices and this integration minimized the malware growth on this stage. There is a tremendous increase on IP-based sensors and this leads to attack the data. These evolvements in technology highlight the need for new identification techniques and coining new security protocols. The revised structure should be applied to endpoint IoE devices within the cross culture communication in accordance with their enhanced capabilities. It is clear that IoE always leverages new challenges to security architects and networks. There is a need to evolve smart security systems which include predictive analysis, anomaly detection and threat detection for cross-culture communications.

References

[1] Bekkering, Ernst and J.P. Shim. (2016) "i2i Trust in Videoconferencing." Communications of the ACM 49.7 103-107. 8.

[2] Boh, W. F., & Yellin, D. (2006). Using Enterprise Architecture Standards in Managing Information Technology. Journal of Management Information Systems, 13(3), 163-207.

[3] Botha, A., Vosloo, S., Kuner, J., & Berg, M. v. (2009). Improving Cross-Cultural Awareness and Communication through Mobile Technologies. International Journal of Mobile and Blended Learning, 39 - 53.

[4] Capgemini. (2016). Securing the Internet of Everything opportunity: putting cybersecurity at the heart of the IoE. Retrieved from capgemini.com: https://www.uk.capgemini.com/resources/securing-the-internet-of-things-opportunity-putting-cybersecurity-at-the-heart-of-the-IoE

[5] D. Miorandi, S. Sicari, P. De, and I. Chlamtac. (2012) Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516.

[6] Fruchter, R, Chen, M, Ando, C. (2003) Geographically Distributed Teamwork Mediated by Virtual Auditorium, Proc. of SID2003 2nd Social Intelligence Design Symposium, ed. D. Rosenberg, T. Nishida, R. Fruchter, London, UK.

[7] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Everything (IoE): A vision, architectural elements, and future directions. Future Generation Computer Systems, 1645 - 1660.

[8] H. Ning and S. Hu. (2011) Technology classification, industry, and education for future Internet of Things. International Journal of Communication Systems, 25(9), 1230-1241.

[9] Järvenpää, S.L., Tractinsky, N. (1999): Consumer Trust in an Internet Store: A Cross-Cultural Validation. Journal of Computer-Mediated Communication, Vol.5 (2), December 1999, available online at http://www.ascusc.org/jcmc/.

[10] K, Karimi. (2014) What the Internet of Things (IoT) needs to become a reality. Available http://www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf, [Accessed 24 January, 2016]

[11] L. Tan and N. Wang. (2010) Future Internet: The Internet of Things. Advanced Computer Theory and Engineering (ICACTE), 5(1), 376-380.

[12] Lam, W. (2005) Investigating success factors in enterprise application integration: A case-driven analysis. European Journal of Information systems, 14(2), 175-187.

[13] Martin, N. L., Pearson, M., & Furumo, K. (2007). IS Project Management: Size, Practices and The Project Management Office1,2. The Journal of computer Information Systems, 47(4), 52-60.

[14] Metastorm (2008). Metastorm releases enhanced ProVision enterprise modeling suite. http://www.metastorm.com/news/2008/040208.asp

[15] R. Weber. (2010) Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30.

[16] Ross, J. W. (2003). Creating a strategic IT architecture competency: learning in stages. MIS Quarterly Executive, 2(1), 31-43.

[17] Sherwood, J. (2005). Enterprise security architecture: a business-driven approach. San Francisco: CMP Books.

[18] Samovar, Larry A., Richard E. Porter, and Edwin R. McDaniel.(2005) Intercultural Communication: A Reader. Thomson Wadsworth.

[19] S. Gaglio and R. Lo(2012). Advances onto the Internet of Things: How ontologies make the Internet of Things meaningful. Cham: Springer.

[20] X. Su, J. Riekki, J. Nurminen, J. Nieminen, and M. Koskimies. (2014) Adding semantics to Internet of Things.