EasyChair Preprint

№ 8012

A Conceptual Framework for Securing IoT-BIM

Baydaa Hashim Mohammed, Hasimi Sallehuddin, Nurhizam Safie, Afifuddin Husairi Bin Hussain and Fadele Ayotunde Alaba

May 22, 2022

A Conceptual Framework for Securing IoT-BIM

Baydaa Hashim Mohammed [1], [2*], Hasimi Sallehuddin[3], Nurhizam Safie[4], Afifuddin Husairi[5] , Fadele Ayotunde Alaba[6]

[1,3,4,] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia.
[2]Departmenrt Computer Techniques Engineering, AL-Esraa University College, Baghdad, Iraq.
[5]Pusat Citra Universiti Universiti Kebangsaan Malaysia (UKM) 43600 Bangi, Selangor, Malaysia.
[6]Department of Computer Science, Federal College of Education, Zaria, Kaduna State, Nigeria.

Corresponding authors: (baidaa81@gmail.com)/(baydaa@esraa.edu.iq)

Funding: This research was fully funded by Universiti Kebangsaan Malaysia and the Ministry of Higher Education Malaysiafor financially supporting this research (FRGS/1/2020/TK0/UKM/02/9).

Abstract

Recently, the Internet of Things and building information modeling (IoT-BIM) has captured attention because of its wide range of applications in multiple domains communicating across different layers. The IoT-BIM consists of three layers, namely physical, network, and application layer. This paper provides and discusses security attacks countermeasure for each IoT-BIM layer. In this paper, we discuss various state-of-the-art IoT-BIM security frameworks and propose a unified security framework for IoT-BIM networks, called "Unified Federated Security Framework". The proposed framework relies on fuzzy cognitive maps for modeling and evaluating trust relationships between the involved entities in federated identity management systems.

Keywords: *IoT, BIM, Security, Framework, Attacks*

1. Introduction

The Internet of Things (IoT) and big data applications are set to play a critical role in increasing global agricultural production to feed billions in the next decades [1]. Experts predict a data-driven future in which farmers will be able to feed the globe thanks to sensors on agricultural equipment, self-driving tractors, drones, and GPS imagery [2]. This would enable communities to deal better with restricted fossil energy, water, and available land supplies. Building Information Modelling (BIM) is a universal phenomenon that can affect the evolution of the built environment. BIM is the technical breakthrough required to modernize the construction industry [3]. A broad range of participation from all project participants is required for a successful transition to BIM adoption [4].

BIM is a digital depiction of a facility's physical and functional attributes that serves as a common knowledge resource for data about it. By definition, the engineering consulting services (ECS) industry cannot use BIM in isolation and must collaborate with other major players [5]. BIM has the potential capability to be considered a disruptive technology whereby it can supplant existing technology, such as 2D CAD. Certain issues regarding BIM's application in real-world environments suggest the immature technology lacks refinement and has performance problems. As pan-project BIM capability matures, the benefits of 4D, 5D, 6D modelling will emerge (Sacks et al., 2010).

The IoT-BIM enables different devices/objects around us to communicate with each other by injecting powerful codes into the devices [6]. IoT-BIM comprises physical objects such as sensors, actuators, mobile phones, and Radio Frequency Identification (RFID) tags, which can sense, monitor, communicate and exchange data with each other to perform different tasks around a specified location. IoT-BIM provides interconnection of various types of devices over possibly vast heterogeneous networks so that the devices can communicate directly with each other without human intervention (Hossain, Islam, Ali, Kwak, & Hasan, 2018). The growth and development in smart have made IoT-BIM gain attention from various research groups, system developers, and industries, and thus, many kinds of service applications have been proposed and developed. However, presently, the demand for large-scale deployment of IoT-BIM devices is increasing rapidly, resulting in a major security concern.

Security is one of the critical features of any communication network. The nature of wireless

networks makes them more susceptible to security attacks. The constraints (e.g., limited processing power) inherent in IoT-BIM devices limit their ability to defend themselves from attacks. For many years, security is one of the critical aspects of any communication network and attacks have targeted wired networks. With the advances in technology, wireless networks are becoming more affordable and easier to build, and attacks on wireless networks have only recently become widespread [8]. A lack of a unified security framework is a major security challenge in an IoT-BIM environment [8] and [9]. Securing IoT-BIM architecture/framework is a significant challenge that needs proper attention for IoT-BIM to be fully adopted [10] [11]. Because presently, there is no universally accepted IoT-BIM framework, making IoT-BIM devices vulnerable to attacks and threats. For that reason, security is a significant challenge that needs proper attention for IoT-BIM to be fully embraced.

There are several benefits to implementing IoT-BIM in the construction industry. These include improved execution monitoring, effective control, higher quality, lower costs, and shorter turnaround times. Because of the availability of real-time data analytics, it has also been broadened to be utilized in making quick decisions. The introduction of new technology is fraught with difficulties, which may be divided into three categories: method of introduction, lack of acceptability, and lack of knowledge and experience.
This study intends to explore building stakeholders' awareness of IoT-BIM application and relevance; it then analyzes the problems of implementing IoT-BIM in construction projects; and lastly, it determines the prevailing challenges of implementing IoT-BIM in the construction field.
This paper provides detailed state-of-the-art IoT-BIM security frameworks and attack countermeasures for IoT-BIM network and also propose a unified security framework which is based on “User identification” for IoT-BIM network called unified federated security framework.
This paper is organized as follows. Section 2 discusses the state-of-the-art IoT-BIM attacks framework. Section 3 presents the proposed unified security framework for IoT-BIM. Section 4 provides the conclusions.

2. State-of-the-Art IoT-BIM Security Framework

Although researchers have proposed frameworks that support various IoT-BIM constrained devices based on identity certificate management, single sign-on, federated identity, and user-centric framework, each framework has its limitation in terms of functional performance. Moreover, most of the existing frameworks have focused on developing individual attack frameworks for physical, network, and application layers of the IoT-BIM. For example, [12] and [13] introduced Public Key Infrastructure and Pretty Good Privacy (PGP), both using identity certificate management. However, the frameworks do not support functions like single sign-on, federated identity, user-centric, and device security. Similarly, [14] introduced Kerberos using single sign-on, but the framework does not support other functions like identity certificate management, federated identity, user-centric, and device security. In addition, [15] introduced a liberty alliance. The framework has functional features such as single sign-on, federated identity, and user-centric, but does not support functions like identity certificate management and device security. Note that among all the existing frameworks, there is no framework for device security. Furthermore, [4], [16] proposed a security framework for smart cities that comprises of Black Networks and Key Management System (KMS) that tackle attacks vulnerabilities at IoT-BIM application layer. The framework provides confidentiality, integrity and privacy, and efficient key distribution. It aims to provide security procedures that will reduce the vulnerabilities in IoT-BIM at the application layer. However, the framework cannot provide robust security for smart city IoT-BIM devices because it is susceptible to side-channel attacks, cryptanalysis attacks, denial of service (DoS) attacks and malicious scripts.
Similarly, [17] suggested an unique SDN-based security architecture for IoT-BIM physical layer that employs border controllers to safeguard voice over IP (VoIP) architectures while allowing interworking between incompatible signaling messages and media flows across IoT-BIM devices The framework integrates heterogeneous IoT-BIM devices from multiple domains, improves the security of each domain, and allocates security guidelines by harming the protection of any domain. However, the challenge with the use of border controllers is on how to secure

traffic (wanted and unwanted). Moreover, data forging, side-channel attacks, traffic diversion, traffic sniffing, DoS, identity spoofing, firmware exploitations are possible attacks associated with SDN, which leads to major problems, such as packet delay/loss and DDoS.

[18] proposed the Object Security Framework (OSCAR), a middleware framework primarily for End-to-End (E2E) security at the IoT-BIM network layer, with constrained application protocol support (CoAP). The method allows multicasting, asynchronous data transmission, and caching. With the simple Datagram Transport Layer Security (DTLS) technique, it addresses E2E security and permission issues while ensuring full data integrity. Failure in the node that functions as a PAN coordinator in beacon-enabled 802.15.4 (i.e., the technical standard that specifies the operation of low-rate wireless personal area networks (LR-WPANs)) affects the intermittent transmission of beacons in the network. Also, [19] discussed different IoT-BIM security challenges that exist in the three-layer system framework and developed a solution to tackle this security threat. The authors identify security challenges in every layer of the IoT-BIM framework.

None of the current security frameworks guarantee comprehensive security for the whole IoT-BIM network; instead, they target/focus on a specific layer of the network. Because there's not a comprehensive IoT-BIM security architecture, communication technologies including WSN, RFID, WiFi, and 4G and 5G are vulnerable to various attacks [20]. It also exposes the data in the communication channels to risks such as eavesdropping, MitM, and counterfeit (Fadele *et al.*, 2018). This study aims to propose a federated unified security architecture with comprehensive security features for IoT-BIM networks. It also gives an accurate classification of all assaults, capturing all forms of threats so that better defenses may be designed and deployed.

3. Proposed Unified Security Framework for IoT-BIM

This section presents a conceptual unified federated security framework for IoT-BIM. It discusses an attempt towards unifying IoT-BIM security framework and preventing IoT-BIM devices/systems from attacks and threats at different layers of the network. The proposed framework is based on “User identification”.

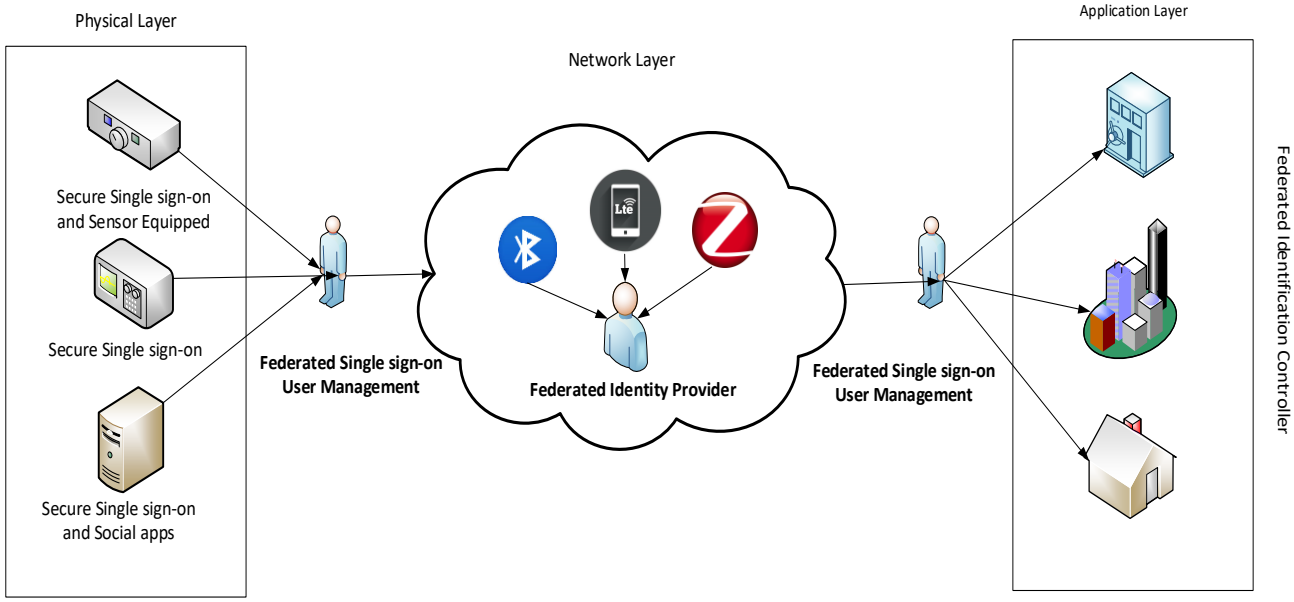

Figure 1: A Unified Federated Security Framework for IoT-BIM Network Scenario

.

Figure 1 depicts a suggested unified federated security framework scenario for an IoT-BIM network based on device identification and taking into account the three levels of IoT-BIM. Users from one IoT-BIM layer (security layer) can access resources from another security layer using the proposed federated identity-based system. The structure is built on the three tiers' mutual trust. Using Fuzzy Cognitive Maps to assess each other's trust (FCMs). FCMs have shown to be a practical, easy-to-use, and powerful qualitative tool for modeling and computing trust in complex and dynamical environments [16], [22].

In this example, users register their credentials with the authentication server in the physical layer, while the other tiers trust its claims. Because it can maintain a user's identity across many security domains on the web, federated identities are a popular solution in online security for safeguarding system workflow. The federated identity idea for unified IoT-BIM security has not been investigated in the context of IoT-BIM [18], [23], [24]. While delivering authentication services to depending tiers and applications in the network, the federated identity provider produces, maintains, and manages device identity information. We investigate the notion in IoT-BIM networks, primarily because the system workflow typically requires a legitimate user (device) to be verified in many domains.

It should be noted that the federated identity framework IoT-BIM is different from web-based [24]–[27]. The communication among identities (nodes) in IoT-BIM is in the form of device-to-device (D2D) communication while in the web-based system, it is known as a person's identity [28]. A detailed communication process in the proposed framework is presented in Figure 2.

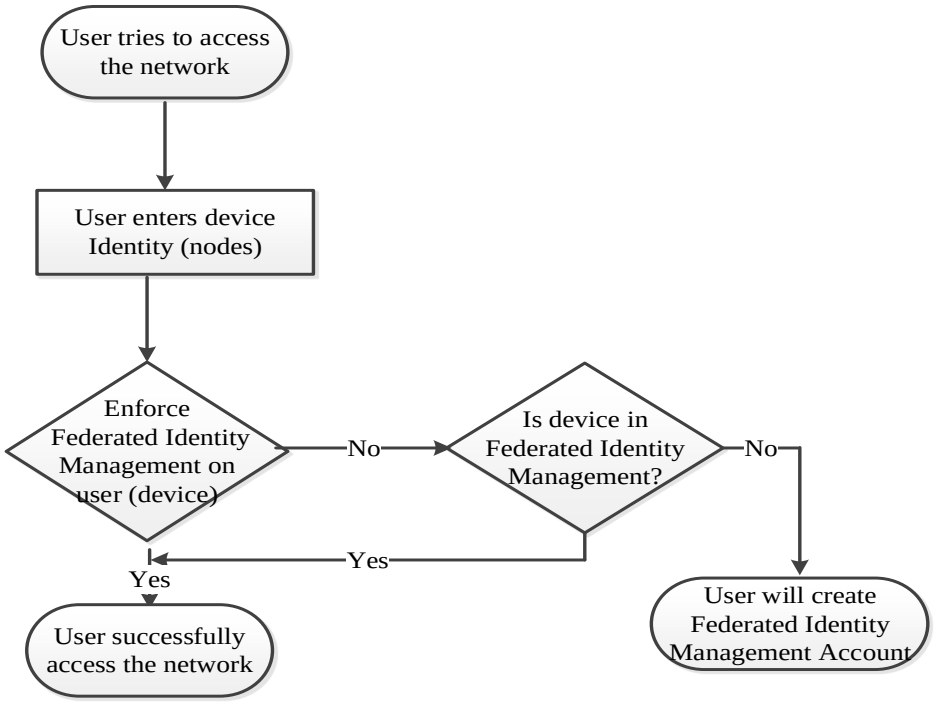

Figure 2: Federated Identity Management Process

The working processing of trust computation different layers is based on fuzzy weighted digraph. It consists of a set $(X1, X2, \ldots, Xn)$ of n interconnected nodes representing variable of communicating nodes of the modeled system for IoT-BIM network such as inputs, outputs, states, events, and signed weighted arcs which describe the causal relationships between these nodes and interconnect them. However, the value of each node is computed from the influence of other nodes to the specified node, by applying the calculation rule in Eq. (1).

$$Y_i^{(t+1)} = V\left(Y_i^{(t)} + \sum_{j=1\ J\neq i}^{n} Y_j^{(t)} * W_{ji}\right) \quad (1)$$

Where, $Y_i^{(t+1)}$ is the value of communicating nodes X_i at time step t + 1. $Y_i^{(t)}$ is the value of communicating nodes X_i at time step t. W_{ji} is the edge weight that interconnects the layers together. It is a given value on the interval [−1, 1] to indicate three possible types of relationships among the layers. V is the threshold or activation function for converting the output of each computation to the range [0, 1] or [−1, 1].

4. Conclusion

Research in IoT-BIM has attracted much interest in the past decade with a great potential to transform human lives and activities. Currently, there is little research on securing an IoT-BIM network from attacks, which makes the dream of achieving a unified security framework for IoT-BIM unrealistic. Thus, it is imperative to address the security attacks in IoT-BIM, which will assist in achieving a unified security framework. An attempt towards unifying the IoT-BIM framework is provided in this study by proposing a unified federated security framework for IoT-BIM and discussing the IoT-BIM security countermeasure for each layer in the framework.

5. Reference

[1] P. Jayashankar, S. Nilakanta, W. J. Johnston, P. Gill, and R. Burres, "IoT adoption in agriculture: the role of trust, perceived value and risk," *J. Bus. Ind. Mark.*, vol. 33, no. 6, pp. 804–821, 2018, doi: 10.1108/JBIM-01-2018-0023.

[2] G. Rajendran, R. S. Ragul Nivash, P. P. Parthy, and S. Balamurugan, "Modern security threats in the internet of things (IoT): Attacks and countermeasures," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019-Octob, 2019, doi: 10.1109/CCST.2019.8888399.

[3] J. Rogers, H. Y. Chong, and C. Preece, "Adoption of Building Information Modelling technology (BIM): Perspectives from Malaysian engineering consulting services firms," *Eng. Constr. Archit. Manag.*, vol. 22, no. 4, pp. 424–445, 2015, doi: 10.1108/ECAM-05-2014-0067.

[4] Y. Al-Saeed, D. J. Edwards, and S. Scaysbrook, "Automating construction manufacturing procedures using BIM digital objects (BDOs): Case study of knowledge transfer partnership project in UK," *Constr. Innov.*, vol. 20, no. 3, pp. 345–377, 2020, doi: 10.1108/CI-12-2019-0141.

[5] L. Kulle, "Intrusion Attack & Anomaly Detection in IoT using Honeypots," 2020.

[6] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 32–37, 2017, doi: 10.1109/I-SMAC.2017.8058363.

[7] M. Hossain, S. M. R. Islam, F. Ali, K. S. Kwak, and R. Hasan, "An Internet of Things-based health prescription assistant and its security system design," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 422–439, 2018, doi: 10.1016/j.future.2017.11.020.

[8] N. Namvar, W. Saad, N. Bahadori, and B. Kelley, "Jamming in the internet of things: A game-theoretic perspective," *2016 IEEE Glob. Commun. Conf. GLOBECOM 2016 - Proc.*, 2016, doi: 10.1109/GLOCOM.2016.7841922.

[9] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014, doi: 10.1007/s11276-014-0761-7.

[10] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 3–16, 2015, doi: 10.1016/j.adhoc.2014.12.005.

[11] and F. H. Ramão Tiago Tiburski, Leonardo Albernaz Amaral, Everton de Matos, "T He I Mportance of B Eing," vol. 44, no. 0, pp. 95–128, 2015, doi: 10.3732/ajb.0800322.

[12] G. Huston, G. Michaelson, and S. Kent, "Resource certification - A public key infrastructure for IP addresses and AS's," *2014 IEEE Globecom Work. Gc Work. 2014*,

2014, doi: 10.1109/GLOCOMW.2009.5360715.

[13] T. Guneysu and T. Oder, “Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things,” *2017 18th Int. Symp. Qual. Electron. Des.*, pp. 319–324, 2017, doi: 10.1109/ISQED.2017.7918335.

[14] B. C. Neuman and T. Ts’o, “Kerberos: An Authentication Sevice for Computer Networks,” *IEEE Commun. Mag.*, vol. 32, no. September, pp. 33–38, 2014, doi: 10.1109/35.312841.

[15] M. I. Chehab and A. E. Abdallah, “Architectures for identity management,” *Internet Technol. Secur. Trans. 2009. {ICITST} 2009. Int. Conf.*, pp. 1–8, 2016, doi: 978-1-4244-5647-5.

[16] K. C. Dahanayake and N. Sumanarathna, “IoT-BIM-based digital transformation in facilities management: a conceptual model,” *J. Facil. Manag.*, 2021, doi: 10.1108/JFM-10-2020-0076.

[17] H. R. Abed, W. A. Hatem, and N. A. Jasim, “Adopting BIM Technology in Fall Prevention Plans,” *Civ. Eng. J.*, vol. 5, no. 10, pp. 2270–2281, 2019.

[18] C. Pu and K. K. R. Choo, “Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function,” *Comput. Secur.*, vol. 113, p. 102541, 2022, doi: 10.1016/j.cose.2021.102541.

[19] B. H. Mohammed, N. Safie, H. Sallehuddin, and A. H. Bin Hussain, “Building Information Modelling (BIM) and the Internet-of-Things (IoT): A Systematic Mapping Study,” *IEEE Access*, vol. 8, no. August, pp. 155171–155183, 2020, doi: 10.1109/ACCESS.2020.3016919.

[20] J. Zenkert, M. Dornh, C. Weber, C. Ngoukam, and M. Fathi, “Big Data Analytics in Smart Mobility : Modeling and Analysis of the Aarhus Smart City Dataset,” pp. 363–368, 2018, doi: 10.1109/ICPHYS.2018.8387685.

[21] A. A. Fadele *et al.*, “A novel countermeasure technique for reactive jamming attack in internet of things,” *Multimed. Tools Appl.*, vol. 23, no. 34, pp. 23–41, 2018, doi: 10.1007/s11042-018-6684-z.

[22] K. Bendiab, S. Shiaeles, S. Boucherkha, and B. Ghita, “FCMDT : A novel fuzzy cognitive maps dynamic trust model for cloud federated,” vol. 86, pp. 270–290, 2019, doi: 10.1016/j.cose.2019.06.011.

[23] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, “Capability-based Access Control Delegation Model on the Federated IoT Network,” *IEEE Trans. Mob. Comput.*, vol. 5, no. 3, pp. 604–608, 2014.

[24] G. H. C. de Oliveira, A. de Souza Batista, M. Nogueira, and A. L. dos Santos, “An access control for IoT based on network community perception and social trust against Sybil attacks,” *Int. J. Netw. Manag.*, vol. 32, no. 1, pp. 1–21, 2022, doi: 10.1002/nem.2181.

[25] H. Yi and Z. Nie, “Side-channel security analysis of UOV signature for cloud-based Internet of Things,” *Futur. Gener. Comput. Syst.*, vol. 86, pp. 704–708, 2018, doi: 10.1016/j.future.2018.04.083.

[26] Y. Liu, H. Wang, T. Li, P. Li, and J. Ling, “Attribute-based handshake protocol for mobile healthcare social networks,” *Futur. Gener. Comput. Syst.*, vol. 86, pp. 873–880, 2016, doi: 10.1016/j.future.2016.12.010.

[27] G. Desogus, E. Quaquero, G. Rubiu, G. Gatto, and C. Perra, “Bim and iot sensors integration: A framework for consumption and indoor conditions data monitoring of existing buildings,” *Sustain.*, vol. 13, no. 8, 2021, doi: 10.3390/su13084496.

[28] G. Sun, D. Liao, S. Bu, H. Yu, Z. Sun, and V. Chang, “The efficient framework and algorithm for provisioning evolving VDC in federated data centers,” *Futur. Gener. Comput. Syst.*, vol. 73, pp. 79–89, 2017, doi: 10.1016/j.future.2016.12.019.