ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

International Journal of Mechanical Engineering

A PRIVACY-AWARE AUTHENTICATION AND SECURITY ANALYSIS BASED ON MULTI-SERVER PROTOCOL USING BLOCKCHAIN AS ONTOLOGY

[1]M. PRAVEEN KUMAR, [2]DR. T. SWARNALATHA

[1]Research Scholar, Shri Venkateshwara University, Rajabpur Gajraula, Amroha, U.P, India.

[2]Professor, Department of CSE, RSR Engineering College, Nellore, Andhra Pradesh, India.

ABSTRACT: The Physical Unclonable Functions (PUFs) has been emerged as a prospective primitive for providing IoT nodes (INs) with less weight physical identities to authenticate the architectures of Cloud-Edge (CE) and Internet of Things (IoT). While injecting PUFs into multi-server authenticating protocols certain security issues can be face that requires to be analyzed for addressing vulnerabilities in architecture design but it is an error-prone task, particularly in complex systems which are applying Block Chain (BC) technology. In this paper a privacy-aware authentication and security analysis based on multi-server protocol using block chain as ontology is presented. In this first the real correlations of CRP (Cloud Resource Providers) can be double-encoded into MCs (mapping Correlations) through a one-time physical identity and a function of keyed-hash. The Block Chain has leveraged for storing MCs and effectively synchronizes them. After that formal security analysis is performed in such software architectures based on Block Chain combines ontology reasoning and model checking methods. Formally this presented protocol security is proved through oracle model and security features have been discussed for exhibiting this protocol can resist different attacks. The results analysis present that the framework presented in this will accommodates authenticated CE-IoT systems then would automatically identifying particular security vulnerabilities and generating informative conditions which represents how attacks will impact the Block Chain.

KEY WORDS: PUFs, CE- IOT, CRPs, MCs, block chain, Ontology.

I. INTRODUCTION

Privacy and security have become significant issues preventing the developments in CE-IoT systems. Often these smart devices have been deployed in open areas and suffering from physical attacks, cloning. What is worse, the communication among these servers and devices is established in a public channel, in which private and sensitive data is exposed by malicious attackers [1]. The authentication plays a vital role for enhancing multi-server CE-IoT system security and privacy is evident that it will verify communications identity effectively, mutually and established a trustworthy session key for protecting the public channel. Due to the rapid development information techniques and networks, several services and application based on internet platforms have been emerging one by one [2]. Due to this, two-third of users tends to reuse the same passwords and identities for multiple services or applications for making them memorizing simpler [3]. However this type of brings more convenience to users in addition it comes with a potential security risk. The multi-server authentication technique is a effective solution for addressing the barrier that only requires users for registering once at the registration center (RC). The technology of Multi-server authentication has becoming most popular with extensive networking applications. However it has brought greater convenience for people’s life, security becoming a significant problem and attracts numerous attentions in industry and academia [4].

From the past two decades, a series of multi-server authentication techniques without the support of online RC utilizing cryptography of self-certified public key was presented for enhancing security [5]. Though it may leads to single-point issue because of centralized architecture. Rather, the facility of user revocation is not resolved in these kinds of approaches. As known that the technology of block chain has huge advantages and brought a promising solution to the issues of user revocation and single failure compared to classical cryptography technologies. The block chain technology emergence has obtained a novel solution for key agreement and authentication technique in multi server structure. This block chain technology is tamper-proof, decentralized and maintained jointly through multiple parties [6]. This technology will solves the trust issue between servers and users and provides better robustness to multi-server systems and avoids above mentioned risks of security. The Block Chain is utilized to enforce the network systems security is proved as beneficial significantly. Here an idea and Block Chain technology is applied for constructing a privacy-awareness authentication technique to a multi-server domain. During design stage an analysis technique is aiming to verify security as a non-functional requirement then design is compiled with functional necessaries.

II. LITERATURE SURVEY

The work [7] implemented a decentralized structure based on Block Chain and a collection period of dynamic transaction for ensuring mutual authentication and distributed key management simplification in heterogeneous vehicular communication systems. Wan et al. [8] noticed that Chuang et al.'s technique can't guaranteed anonymity and cannot resisted loss attacks of smart card, hence they presented an enhanced technique that will solve the issues in earlier scheme as well as inheriting merit of actual approach. In 2015, He and Wang [9] presented a robust multi server authentication technique depends on biometric that has truly first 3-factor authentication technique to the environment of multi-server. Fuzzy extractor is utilized for extracting biometric key from biometric data. Odelu et al. [10] has point out that He and Wang's technique was vulnerable for known session-specific temporary data attacks and impersonation attacks.

The paper [11] describes the present problems and possible solutions with the development of ontology in the interaction of human-robot. This work evaluated ontologies role in robotics at huge, obtains a overall service robot ontologies review described standards to robots with future models in the environment and defined present problems and possible solutions with the development of ontology for the interaction of human-robot. In [12] discussed about combining mobile robots and wireless sensor networks. Here authors suggested a layered swarm framework to the decentralized self-organizing complex adaptive systems interaction with mobile robots like a members. Their framework contains 2 layers (Wireless LAN, robots) and communication channels between and within layers. While verifying the framework experimentally mobile robots reached the destination independently.

Wang and Liao et al. [9] presented remote user authentication protocol based on dynamic identity utilizing smart cards for achieving anonymity of users. Their protocol only utilizes hash function for implementing a strong authentication in multi-server domain. A secure technique is provided for updating the password of user's with no trusted third party help. While Wang's and Liao protocol is determined as susceptible to malicious user attacks and malicious server attacks. Shih and Hsiang [14] determined that Wang's protocol is not reparable and susceptible to masquerade attack, registration center spoofing attack, insider attack, server spoofed attacks. But it won't give mutual authentication.

Yang et al. [15] presented a similar type of two-server model to the authentication of user. Various trust levels are assigned to service provider and servers in the presented protocol, mostly server is exposed to users than the control server. Directly back-end control server is not accessible to the clients so that it was less likely to be attacked. Flexibility is provided by Two-server model for distributing the passwords of user and the functionality of authentication in to two servers for eliminating the major vulnerable point of single server approach. Hence two-server approach appears as a reasonable selection to practical applications.

III. PRIVACY-AWARE AUTHENTICATION AND SECURITY ANALYSIS USING BLOCKCHAIN

3.1 Block chain (BC)

This BC becomes a novel distrusted application that plays a trustworthy role in decentralized database. Whole data is recorded in transactions form. These transactions can fill a new block after being verified through all participants and these transactions would build a new block, in that block these are recorded permanently in BC. All the authorized nodes have ability for querying or invoking the smart contract for managing the information presented in the database of BC. In this protocol a public ledger is maintained by BC for recording MCs of CRPs to INs. Further in this protocol a Consortium BC is employed for IoT conditions, since it has ability for reaching a consensus with less cost and higher efficiency.

3.2 PUFs

A circuit unique microstructure realizes a PUF instance that is an essential one-way function and constructs correlations among CRPs. The correlation can be indicated as0,1$\}^n$ $\{0,1\}^m$, that generates arbitrary response of m-bits and accepts the n- bit challenge. The PUF is efficient for constructing but hard to predict, clone is due to the physical characteristics of PUF. A fuzzy extractor is utilized for generating the helper information to a particular challenge response pair. The procedure of generation is represented as$(R, HLP) = PUF_{gen}(C)$, here C, R from a CRP and HLP is the helper information. In noisy domains PUF original response can be corrected through fuzzy extractor with helper information support. The process of recovery can be represented as $R = PUF_{rec}(C, HLP)$.

3.3 Multi-Receiver Encryption (MRE)

The MRE is presented for broadcasting an encrypted message to a receiver's subset. The receivers which are belonging to authorized subset only will decrypt the cipher text. Because of this property MRE is included in presented protocol for sharing a dynamic hash key between different servers. For facilitating MRE algorithm is utilized to an S authorized set of n receivers.

MRE Setup (n): First a G bilinear group prime order P is selected with a generator g$\in\mathbb{G}$. Next it chooses 2 random parameters $\alpha, \gamma \in \mathbb{Z}$ and calculated as $v = g' \in \mathbb{G}$. The public key is computed as

$$PK = (g, g_1, \dots, g_n, g_{n+1}, \dots, g_{2n}, v\,) \text{ ---- (1)}$$

where n is the number of receivers, $g_i = g^{\alpha^i}$. The private key for every receiver is $d_i = g_i^v \in \mathbb{G}$. All the materials of key can be shared through a secured channel and transmitted to authorized receivers. The MRE private keyd_i is indicated asK_{MRE} in later part of the paper for avoiding confusion with verifier private key.

(b) MRE Encrypt (PK, S): The sender can select $t \in \mathbb{Z}_p$ utilizes bilinear pairing for computing $K = e(g_{n+1}, g)' \in \mathbb{G}_T$ & $Hdr,$ here K is secret message, prepared as sheared through MRE and Hdr is MRE header given as

$$Hdr = (g^t, (v.\prod_{j\in S} g_{n+1-j})^t) \text{ ------ (2)}$$

Then, encryption output is $(Hdr, K) = MreEn(PK, S),$ here S is authorized set of n receivers.

(c) MRE Decrypt (S, PK, Hdr, $\boldsymbol{d_i}$): Authorized i^th^ receiver will utilize the $\boldsymbol{d_i}$ private key, $Hdr = (C_0, C_1)$ recovering the K message. Decryption can be carried out as

$$K = e\,(g_i, C_1)/e(d_i \cdot \prod_{j\in S} g_{n+1-j+1}, C_0) \text{ --- (3)}$$

At last receiver attains $K = MreDe(S, PK, Hdr, d_i).$

3.3 System Model

Figure.1 represents the system in which presented protocol designed; it contains BC, RC, verifiers and IoT nodes (INs). The formal security analysis also included in this software architecture based on block chain combined with ontology reasoning and model checking schemes. The overview of this authentication protocol integrates 5 major phases. The system setup where RC produces public metrics, initialized the MRE algorithm with all verifiers and initiates BC system. Then these authorized verifiers joined in BC network, the smart contract can be deployed in verifiers and RC for providing four different functions. These 4 functions are utilized for managing MCs through maintaining a persistent database in model checker and attack phases. In the phase of registration RC produces key pairs to INs, verifiers and constructing 1 MC for 1 CRP selected randomly from received CRPs transmitted through IN. The MC would be registered in BC and CRPs are stored in local database of RCs. The session key and mutual authentication can be accomplished between one of authorized verifiers and IN. Finally RC has priority for revoking, re-registering or regulating the verifiers, INs.

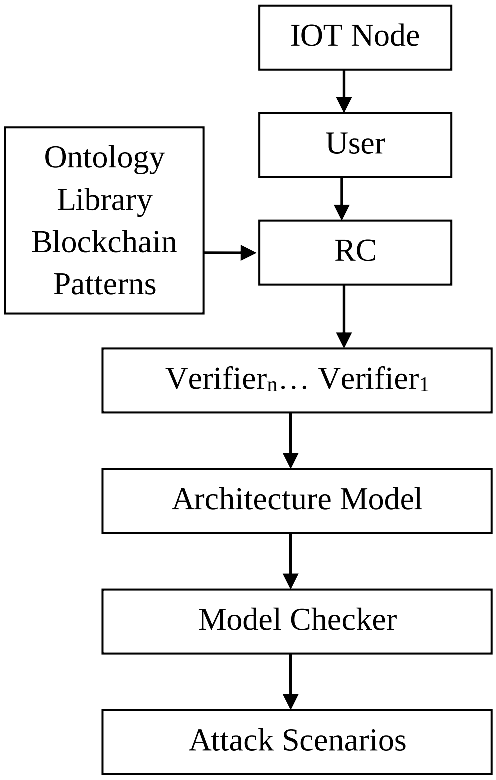

Fig. 1: SYSTEM MODEL OF BLOCKCHAIN BASED PRIVACY-AWARE MULTI-SERVER AUTHENTICATION MODEL

IoT nodes (INs): The INs presented in presented scheme can be defined as smart devices in extending IoT system that does not refer for less weight devices and can]t be applied to extended IoT environments includes smart grid system, IoV (Internet of Vehicles), Industrial Internet of Things, etc. Generally these INs consist a communication module, a PUF circuit and having ability for performing the operations of elliptic curve. They might be smart devices like Industrial IoT devices, smart phones, vehicles, etc. that are utilizing sensor chips for directly collecting the data of IoT and exchanging them with several verifiers. Basically the most appropriate one or nearest verifier can be selected.

RC: The RC is a trustworthy security entity that produces key pairs to all participants and initializing MRE to authorized verifiers. Further the RC has ability for invoking smart contract for revoking, registering and re-registering the INs or regulating the verifiers through transmitting transactions.

Verifier: The verifiers might be base stations, automation controllers, servers that are protected physically and rich in resources for authenticating INs, establishing session keys, exchanging data among them or employing storage devices or computation from remote cloud. Every verifier joins the BC for querying, updating MCs and maintaining public ledger in the period of authentication. The verifiers identity and public key must be available in public for all the participants.

BC: The BC has responsibility to act as a database of distributed key-value. The key is unique address of INs in BC and value is 1 MC utilized in authentication. The BC systems which are supposed for reliably utilize the smart contract for maintaining the database which is allowing to be deployed in presented system.

Model checkder: The reasoner of ontology is utilized here for identifying the vulnerabilities of security in the scheme, depending on the architecture patterns and security characteristics description of ontology. These descriptions of ontology can be defined as classes which are placed in the library of ontology. Assertions are injected in to behavioral scheme based on the vulnerabilities of identity. At last model checker processes the assertions against model and security conditions are generated.

Both structure and behaviour of the Structure in architecture design is defined formally as the representation of ontology utilizing OWL (ontology web language). Beside ontology classes support software architecture modeling based on block chain, in addition defines ontology classes to classify the characteristics of security in this model. The three characteristics Defense in depth, least privilege and Attack surface are utilized for calculating parameter values which measure security of system. The two characteristics Data Disclosure and Data Tampering are utilized for trace attack conditions. These kinds of ontology classes are positioned in the library of ontology. Here remaining characteristics are not addressed and are defined through new class inherited in existing classes or capturing various properties conditionally in the definition of class.

Attack Surface: Formally attack surface will be defined as an ontology class which is known as *attack surface* is created with logic for describing the components that can be accessible publicly by internet or public network like public BC. It can also defined as a component is an attack surface when it has a port of incoming communication which blinds for internet link.

2) Least Privilege: An on-chain component in BC based system is taken as vital element. An ontology rule is utilized for choosing the components which can have access to On-chain elements. In SWRL (Semantic Web Rule Language) this rule is defined. Connection between two components is described as: *comp1* and *comp2,* which *comp2* is a BC.

3) Defence in Depth: For classifying the communication it utilizes security controls, defined the ontology classes *InputSantizedCommPort, FirewalledCommPort, AuthorizedCommPort & AuthenticatedCommPort*. As aiming for capturing the components which can have access to BC and applied security controls, *DefenseInDepth* can be defined as a *LeastPriviledge* subset that contains port bounded to incoming secured communication port.

4) Data Disclosure: Data disclosure happens over a connection that transfer information as a plain text on uncrypted protocols like *ftp* and *http*. The *PlainLink* can be defined for representing connectors that communicates by insecure protocols. An ontology class is known as *DataDisclosureConnector* is defined for describing the connector which is vulnerable for data disclosure since it transfers information in plain text.

5) Data Tampering: If information is transmitted on a connector which is vulnerable to data disclosure, in addition data is vulnerable to tamper when the connector is over a communication link which has no input authorization or sanitization. With no input sanitization the information comes from an unknown source, without authorization the data will be altered in transmission.

Security Attack Scenarios Analysis: As the classes of ontology are described previously, the reasoned of ontology will pinpoint that connector is vulnerable for data disclosure and data tampering. This information is utilized for generating attack cases through injecting attacker elements into design model. The components of attacker indicate software components that adversaries usage. Now the LTL (Linear Temporal Logic) assertions can be produced and injected into the behavioral model in ADL. Due to this the model checker is allowed for tracing the components, how they interact with each other according to the request of attackers. Attacker component is added to model and its attack port is connected to vulnerable connector outbound role. The outbound role is utilized in which the request is started for making system responses. The assertion of LTL proves that the attack conditions are created based on the below formula.

$$\blacksquare(\mathrm{attacker.vulconn.outrole.vevnt} \rightarrow \blacklozenge\ \mathrm{targetcomp.inport.cevnt})$$

The *vevnt* indicates the event that is triggered from vulnerable connector (*vulconn*) outbound role (*outrole*). The cevnt indicates indicate event triggered through the component of target (*targetcomp)* which is responding for the request issued by attacker component (*attacker*). This assertion of LTL check either the component of target is eventually invoked always if the attacker made a request.

IV. RESULT ANALYSIS

In this section first time complexity and computation of presented protocol is analyzed. Formally presented protocol security is proved by random oracle technique. At last general security verification technique based on BC ontology can be evaluated its efficiency during the detection of various attack conditions in terms of recall and precision. In this segment time consumption is presented for proving presented authentication protocol efficiency. 1000 requests of distinct consecutive authentication are utilized and experiment results are recorded. Authentication process each segments time consumption changes across a constant and remains as stable. The results exhibiting that presented protocol performance is reliable. Each segments average consumption is mentioned in Table 1.

Table 1: AVERAGE TIME CONSUMPTION OF AUTHENTICATION PROTOCOL

STAGES	TIME (ms)
MRE Decrypt	39.1
MRE Encrypt	64.2
BC Query	73.6
SK Establish	991.8
MCs Update	2182.1
Total Time	3302.9

The overall authentication protocol requires long time that is 3302.9 ms approximately and the query function of BC takes 73.6 ms. Whereas verifier and IN t requires 991.8 ms only for finishing mutual authentication, establishing session key. If session key is accepted then it will be utilized for encrypting IoT information and immediately protecting the public channel. The new MC to the next authentication can be updated through repeatedly invoking the smart contract by verifier till the transaction is recorded permanently in BC for achieving synchronization. However the MCs synchronization time is2182.1 ms in the test of distinct request and requires much time, it would not add additional time to communicators for affecting session key establishment efficiency.

Table 2 represents the statistics if the scenarios are generated depends on identified connectors which are vulnerable for various conditions.

Table 2: SCENARIO GENERATION

Assertion	Scenario	Time	Impact?
#1	Data Tampering	687ms	None
#2	Data Tampering	930 ms	Indirect
#3	Data Tampering	19 ms	Indirect
#4	Data Tampering	565 ms	None
#5	Data Tampering	937 ms	Indirect
#6	Data Tampering	213 ms	Indirect
#7	Data Tampering	5 ms	Direct
#8	Data Tampering	3462 ms	Indirect

It is observed that certain assertions which represent the components of on-chain having indirect impacts (as represented in last column). These components of on-chain are the target connected directly to the vulnerable connectors but they shown a significant impact from attacks as certain segment of request flow leading to them. The time taken by model checker for processing is responsible to this model size. The reasoned of outlook takes 9,123 milliseconds for detecting all 5 characteristics of security. The attack conditions detection performance in terms of recall, precision are represented in Fig. 2 for proving results completeness and soundness.

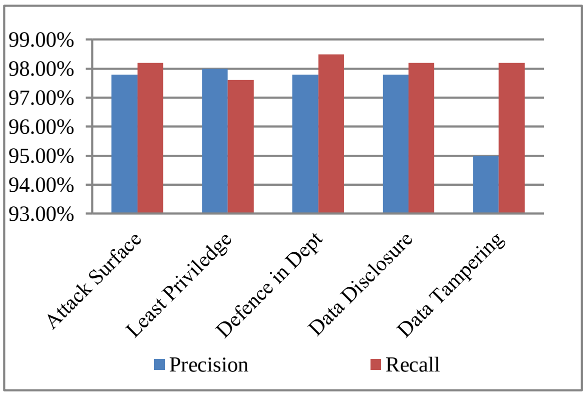

Fig. 2: DETECTION PERFORMANCE OF ATTACK SCENARIOS

From Fig. 2 it is observed that many of detection achieves 98.2% precision and 97.8% recall rate to all characteristics except data tampering since a false-positive (FP) result is determined. While detection accuracy depends on how accurately the characteristics of security can be defined. In addition the design technique required to be checked against the requirements of functional before performing the analysis of security.

V. CONCLUSION

Developed A privacy-aware multi-server PUFs-based authentication protocol using BC in ontology, that is majorly handled with the issues in CE-IoT system while applying PUFs to authentication protocols from multi-servers and attack scenarios are analyzed. Features of security are described for illustrating that the verifiers have ability for accessing the CRPs privacy-aware MCs in BC for authenticating INs without storing the original correlation explicitly and this presented protocol gives key security properties and resists different attacks. Then relying on ontology description of security characteristics and BC architecture pattern, in the design approach vulnerabilities are identified by presented model. The scenarios of attacks are generated according to the identified vulnerabilities utilizing model checking scheme. The results evaluated presented protocol efficiency and takes 2182.1 ms for synchronizing the MCs between verifiers to single request and 991.8 ms for establishing session key. The synchronization technique time is decreased to an effective value whenever receiving the requests of concurrent. These results are determined either the BC has any impact from attacks.

VI. REFERENCES

[1] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography", *J. Netw. Comput. Appl.*, vol. 131, pp. 66-74, 2019.

[2] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications", *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 457-468, Jan 2019

[3] A. Tomar and J. Dhar, "An ecc based secure authentication and key exchange scheme in multi-server environment", *Wireless Personal Communications*, pp. 1-22, 2019.

[4] C. Wang, G. Xu and W. Li, "A secure and anonymous two-factor authentication protocol in multiserver environment", *Security and Communication Networks*, vol. 2018, 2018.

[5] A. K. Das, S. Jangirala and S Mukhopadhyay, "A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards", *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 2735-C2767, 2017.

[6] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in Annual International Cryptology Conference, pp. 357–388, Springer, 2017

[7] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832-1843, 2017, doi: 10.1109/JIOT.2017.2740569.

[8] T. Wan, Z. Liu, and J. Ma, “Authentication and key agreement protocol for multi-server architecture,” Journal of Computer Research and Development, vol. 53, no. 11, pp. 2446–2453, 2016.

[9] D. He and D. Wang, “Robust biometrics-based authentication scheme for multiserver environment,” IEEE Systems Journal, vol. 9, no. 3, pp. 816–823, 2014

[10] V. Odelu, A. K. Das, and A. Goswami, “Cryptanalysis on “robust biometrics-based authentication scheme for multiserver environment”” IACR Cryptology, vol. 2014, 2014.

[11] Haidegger, T.; Barreto, M.; Gonçalves, P.; Habib, M.K.; Ragavan, S.K.V.; Li, H.; Vaccarella, A.; Perrone, R. Applied ontologies and standards for service robots. Robot. Auton. Syst. 2013, 61, 1215–1223.

[12] Li, W.; Shen, W. Swarm behavior control of mobile multi-robots with wireless sensor networks. J. Netw. Comput. Appl. 2011, 34, 1398–1407.

[13] Hsiang HC, Shih WK. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interface 2009;31(6):1118–23

[14] Liao YP, Wang SS. A secure dynamic id-based remote user authentication scheme for multi-server environment. Computer Standards & Interface 2009;31(1):24–9

[15] Yang Y, Deng RH, Bao F. A practical password-based two-server authentication and key exchange system. IEEE Transactions on Dependable and Secure Computing 2006;3(2):105–14