एंड्रॉइड के लिए नियतात्मक सत्यापन

एंड्रॉइड अनुप्रयोगों के लिए व्यावहारिक बहु-चरणीय निर्धारक सत्यापन तकनीक

संपादित : **सी. जे. एंटनी**

मोबाइल अनुप्रयोग प्रायः ऐसे परिवेश में संचालित होते हैं जो केवल आंशिक रूप से विश्वसनीय होते हैं। यद्यपि सर्वर सुरक्षित रहता है, परंतु क्लाइंट डिवाइस उपयोगकर्ता के नियंत्रण में होता है, जिससे आक्रमणकारी एपीके फ़ाइल तक पहुंच प्राप्त करने के बाद अनुप्रयोग का निरीक्षण, संशोधन अथवा स्वचालन कर सकते हैं।

सामान्य सुरक्षा पद्धतियाँ स्थिर क्लाइंट पहचानकर्ताओं, जैसे डिवाइस आईडी अथवा इंस्टॉलेशन टोकन, पर निर्भर करती हैं। इनकी प्रमुख कमजोरी यह है कि ये स्थिर और अपरिवर्तनीय होते हैं। यदि कोई आक्रमणकारी स्थिर आईडी प्राप्त कर ले, तो वह अनिश्चित काल तक क्लाइंट का प्रतिरूपण कर सकता है।

इसके अतिरिक्त, वर्तमान समाधान प्रायः जटिल क्रिप्टोग्राफिक प्रोटोकॉल का उपयोग करते हैं, जिससे संगणनात्मक लागत बढ़ती है तथा एकीकरण कठिन हो जाता है। प्रस्तावित समाधान "निर्धारक व्यवहार" पर आधारित है। इसका अर्थ है कि सर्वर किसी एक स्थिर मान की जांच करने के बजाय समय के साथ क्लाइंट की स्थिति में होने वाले परिवर्तनों के आधार पर उसका सत्यापन करता है।

सुरक्षा जोखिम परिदृश्य और डिज़ाइन लक्ष्य

यह प्रणाली मानती है कि आक्रमणकारी अनुप्रयोग बाइनरी का निरीक्षण कर सकता है, ट्रैफिक की निगरानी कर सकता है तथा अनुरोधों को स्वचालित बना सकता है, परंतु उसे सर्वर-साइड लॉजिक तक पहुंच प्राप्त नहीं होती। उद्देश्य पूर्ण सुरक्षा सुनिश्चित करना नहीं, बल्कि हमले के प्रयास को अत्यधिक कठिन बनाना है।

डिज़ाइन का मुख्य उद्देश्य न्यूनतम डिवाइस प्रभाव के साथ हल्का निष्पादन, याद्दच्छिकता के साथ निर्धारक व्यवहार, सर्वर द्वारा सत्यापनीय स्थिति प्रगति तथा जटिल कुंजी प्रबंधन को समाप्त कर कम परिचालन लागत सुनिश्चित करना है।

क्लाइंट-साइड स्थिति और प्रगति

यह तंत्र क्लाइंट द्वारा बनाए रखी गई अनुक्रम स्थिति पर आधारित है। यह स्थिति एक साधारण पूर्णांक के रूप में प्रदर्शित होती है, जो प्रत्येक सफल इंटरैक्शन के बाद आगे बढ़ती है।

डॉ. अंबाती बुबली सागर
वैज्ञानिक - बी
sagar.ambati@nic.in

एंड्रॉइड अनुप्रयोगों के लिए विकसित यह हल्की निर्धारक सत्यापन तकनीक भारी क्रिप्टोग्राफी पर निर्भर हुए बिना मोबाइल ए.पी.आई. सुरक्षा को सुदृढ़ बनाती है। स्थिर क्लाइंट पहचानकर्ताओं के स्थान पर यह पद्धति एप्लिकेशन के एपीके हस्ताक्षर तथा क्रमिक अनुक्रम का उपयोग करते हुए गतिशील सत्यापन मान उत्पन्न करती है। यह दृष्टिकोण स्टेटलेस सर्वर-साइड सत्यापन को सक्षम बनाता है, रीप्ले हमलों का प्रतिरोध करता है तथा जटिल कुंजी प्रबंधन से बचाव करते हुए सरल बाइट-स्तरीय परिचालनों के माध्यम से संगणनात्मक दक्षता बनाए रखता है। कम ओवरहेड, स्केलेबिलिटी तथा सहज एकीकरण इसे बड़े स्तर पर एंड्रॉइड परिनियोजन के लिए उपयुक्त बनाते हैं।

अनुप्रयोग पुनः प्रारंभ होने पर निरंतरता बनाए रखने के लिए क्लाइंट स्थानीय संग्रहण में न्यूनतम प्रगति संकेतक सुरक्षित रखता है।

यह मान किसी पहचान, प्रमाण-पत्र अथवा संवेदनशील विशेषता का प्रतिनिधित्व नहीं करता। यह केवल निर्धारक सत्यापन अनुक्रम में वर्तमान स्थिति को दर्शाता है। संग्रहित मान का स्वयं में कोई स्वतंत्र सुरक्षा महत्व नहीं है। यदि कोई आक्रमणकारी इसे प्राप्त भी कर ले, तब भी उसे कोई परिचालन लाभ प्राप्त नहीं होता। यदि इसे हटाया, रीसेट अथवा परिवर्तित किया जाए, तो क्लाइंट और सर्वर के बीच अनुक्रम सरेखण बाधित हो जाता है तथा बिना किसी अतिरिक्त सुरक्षा तर्क के सत्यापन स्वाभाविक रूप से विफल हो जाता है।

यह दृष्टिकोण संग्रहित स्थिति को हल्का और गैर-संवेदनशील बनाए रखते हुए परिचालन निरंतरता सुनिश्चित करता है। अनुक्रम केवल अग्रिम दिशा में प्रगति करता है। क्लाइंट सर्वर त्रुटि प्रतिक्रियाओं के आधार पर पुनः-सिंक्रोनाइज़ करने का प्रयास नहीं करता, जिससे नकली अथवा रीप्ले त्रुटि स्थितियों के माध्यम से स्थिति हेरफेर को रोका जा सके।

मान व्युत्पत्ति पाइपलाइन (क्लाइंट)

स्थिर पहचानकर्ता प्रेषित करने के बजाय, क्लाइंट प्रत्येक अनुरोध के लिए निर्धारक बहु-चरणीय प्रक्रिया का उपयोग करते हुए एक नया सत्यापन मान तैयार करता है।

सीड जनरेशन

यह प्रक्रिया एप्लिकेशन के एपीके हस्ताक्षर हैश से प्राप्त आधार सीड से प्रारंभ होती है। इससे यह तंत्र किसी विशिष्ट बिल्ड से संबद्ध हो जाता है। सीड स्थानीय स्तर पर ही सुरक्षित रहता है और कभी प्रेषित नहीं किया जाता।

स्थितिगत निष्कर्षण

सीड का एक छोटा भाग वर्तमान अनुक्रम स्थिति के आधार पर चुना जाता है। जैसे-जैसे स्थिति आगे बढ़ती है, अलग-अलग भागों का उपयोग किया जाता है, जिससे प्रत्येक अनुरोध में विविधता बनी रहती है और साथ ही सर्वर पर उसका पुनरुत्पादन भी संभव रहता है।

रूपांतरण और ऑबफुस्केशन

चयनित भाग पर बिट-स्तरीय रूपांतरण लागू किए जाते हैं, जैसे बिटवाइज रोटेशन तथा एक्सओआर परिचालन, ताकि उसकी प्रस्तुति बदली जा सके। संरचनात्मक अस्पष्टता बढ़ाने के लिए प्रेषित स्ट्रिंग में अतिरिक्त गैर-अर्थपूर्ण वर्ण भी जोड़े जाते हैं। सत्यापन के दौरान इन वर्णों की उपेक्षा की जाती है।

इंटीग्रिटी मार्कर

रूपांतरित भाग से एक चेकसम तैयार किया जाता है। इससे गहन सत्यापन से पहले ही भ्रष्ट अथवा छेड़छाड़ किए गए मानों को अस्वीकार करना संभव हो जाता है।

सर्वर-साइड पुनर्निर्माण

सर्वर स्टेटलेस तरीके से कार्य करता है। किसी मान को प्राप्त करने पर सर्वर डिक्रिप्शन का प्रयास नहीं करता। इसके बजाय, वह अपेक्षित परिणाम का निर्धारक रूप से पुनर्निर्माण करता है।

- **पार्सिंग:** आगत संदेश से एन्कोडेड अनुक्रम स्थिति निकाली जाती है।
- **सीड पुनर्गणना:** एप्लिकेशन हस्ताक्षर की संग्रहीत प्रति का

उपयोग करते हुए सर्वर उसी आंतरिक सीड को पुनः उत्पन्न करता है।

- **सिमुलेशन:** सर्वर अपेक्षित मान प्राप्त करने के लिए समान निष्कर्षण और रूपांतरण चरणों को लागू करता है।
- **तुलना:** प्राप्त मान की तुलना व्युत्पन्न मान से की जाती है। इसके लिए सटीक मिलान आवश्यक होता है।

स्वतंत्र सत्यापन

चूंकि सर्वर आवश्यकता अनुसार सीड की पुनर्गणना करता है, इसलिए उसे क्लाइंट सीक्रेट्स संग्रहित करने की आवश्यकता नहीं होती। प्रत्येक अनुरोध का सत्यापन स्वतंत्र रूप से किया जाता है। यदि अनुरोध वैध होता है, तो उसे स्वीकार कर लिया जाता है; अन्यथा, "गलत अनुक्रम" अथवा "अमान्य चेकसम" जैसे विशिष्ट कारण प्रकट किए बिना उसे अस्वीकार कर दिया जाता है।

सुरक्षा विश्लेषण

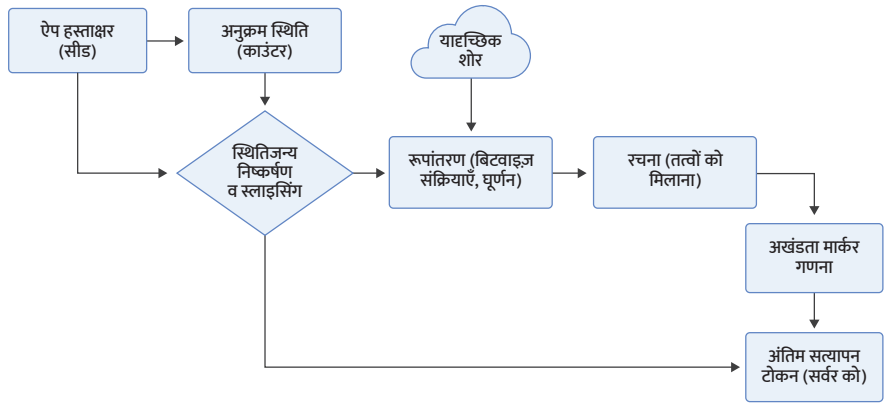
प्रस्तावित तंत्र अपनी शक्ति असममित प्रयास सिद्धांत से प्राप्त करता है।

- **क्लाइंट के लिए:** संगणनात्मक लागत अत्यंत न्यूनतम है। इसमें सरल बाइट रूपांतरण शामिल हैं, जो मानक डिवाइसों पर तीव्र गति से निष्पादित होते हैं।
- **आक्रमणकारी के लिए:** वैध अनुरोध तैयार करने हेतु संपूर्ण आंतरिक व्युत्पत्ति पाइपलाइन की पुनरावृत्ति आवश्यक होती है। साधारण रीप्ले प्रयास प्रभावी नहीं होते, क्योंकि प्रत्येक इंटरैक्शन के साथ अनुक्रम स्थिति आगे बढ़ती रहती है।
- **क्लोनिंग के प्रति प्रतिरोध:** केवल अनुप्रयोग बाइनरी का स्वामित्व पर्याप्त नहीं है। अधिकृत सर्वर-साइड संदर्भ डेटा तथा निर्धारक सरेखण के अभाव में उत्पन्न मानों का सत्यापन संभव नहीं होता।
- **समान विफलता व्यवहार:** सभी सत्यापन विफलताएँ एक समान परिणाम उत्पन्न करती हैं। इससे आक्रमणकारी त्रुटि-आधारित परीक्षण के माध्यम से आंतरिक लॉजिक का अनुमान नहीं लगा सकते।

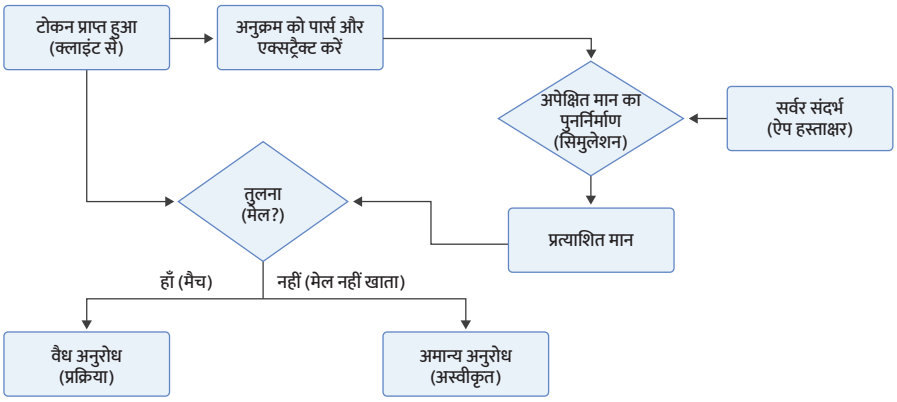
परिचालन एवं परिनियोजन लाभ

अभियांत्रिकी दृष्टिकोण से यह पद्धति बड़े स्तर के परिनियोजन के लिए व्यावहारिक है।

- **स्थिर प्रदर्शन:** सत्यापन लॉजिक निश्चित आकार के बाइट परिचालनों पर आधारित है और प्रत्येक अनुरोध के लिए स्थिर समय ओ(1) में कार्य करता है। उपयोगकर्ताओं की संख्या बढ़ने पर भी प्रदर्शन प्रभावित नहीं होता।
- **डेटाबेस निर्भरता का अभाव:** सत्यापन के लिए प्रति-उपयोगकर्ता डेटाबेस लुकअप की आवश्यकता नहीं होती, जिससे विलंबता तथा सर्वर लोड कम होता है।
- **स्टेटलेस सत्यापन:** प्रत्येक अनुरोध का मूल्यांकन स्वतंत्र रूप से किया जाता है, जिससे क्षैतिज स्केलिंग सरल हो जाती है।
- **ऑफलाइन तत्परता:** क्लाइंट तात्कालिक नेटवर्क पहुंच के बिना भी अपनी प्रगति स्थिति प्रारंभ एवं आगे बढ़ा सकता है।
- **सहज एकीकरण:** यह लॉजिक विशेष अनुमतियों अथवा पृष्ठभूमि सेवाओं की आवश्यकता के बिना मानक अनुप्रयोग वर्कफ़्लो में एकीकृत किया जा सकता है।



▲ चित्र 12.1 क्लाइंट-साइड प्रक्रिया



▲ चित्र 12.2 सर्वर-साइड पुनर्निर्माण

निष्कर्ष

यह कार्य भारी क्रिप्टोग्राफिक आदान-प्रदान पर निर्भर हुए बिना मोबाइल एपीआई सुरक्षा को सुदृढ़ करने हेतु एक व्यावहारिक निर्धारक सत्यापन पद्धति प्रस्तुत करता है। एप्लिकेशन बिल्ड हस्ताक्षर तथा प्रगतिशील आंतरिक अनुक्रम के साथ सत्यापन को जोड़कर यह तकनीक प्रतिरूपण एवं स्वचालित दुरुपयोग के लिए आवश्यक प्रयास को बढ़ा देती है।

इसकी हल्की संगणना, स्टेटलेस सर्वर सत्यापन तथा सरल परिनियोजन इसे बड़े स्तर के मोबाइल परिवेशों के लिए उपयुक्त बनाते हैं, जहाँ प्रदर्शन और परिचालन सरलता अत्यंत महत्वपूर्ण होती है।

▼ तालिका : प्रस्तावित निर्धारक सत्यापन तकनीक और पारंपरिक दृष्टिकोणों के बीच प्रमुख अंतर

विशेषता	स्थिर पहचानकर्ता (जैसे डिवाइस आईडी)	भारी क्रिप्टोग्राफी (जैसे क्लाइंट प्रमाण-पत्र)	प्रस्तावित निर्धारक पद्धति
क्लाइंट पहचानकर्ता	स्थिर एवं अपरिवर्तनीय मान	निजी कुंजी	गतिशील, प्रत्येक अनुरोध के साथ प्रगति करने वाला
रीप्ले सुरक्षा	नहीं (आसानी से पुनः उपयोग संभव)	उच्च (नॉन्स/टाइमस्टैम्प के माध्यम से)	प्रगतिशील अनुक्रम-आधारित टोकनों के कारण पुनः उपयोग अत्यंत कठिन
सर्वर स्थिति	स्टेटफुल (आईडी संग्रहित करनी होती हैं)	स्टेटफुल (प्रमाण-पत्र/कुंजियों का प्रबंधन)	स्टेटलेस (आवश्यकतानुसार पुनर्निर्माण)
संगणनात्मक लागत	अत्यंत कम	उच्च (जटिल गणितीय परिचालन)	कम (बिटवाइज परिचालन)
प्रमुख कमजोरी	चोरी एवं रीप्ले के प्रति संवेदनशील	प्रबंधन और परिनियोजन में जटिल	क्लाइंट बाइनरी लॉजिक जे.एन.आई. तथा ऑबफुस्केशन के माध्यम से संरक्षित

अधिक जानकारी के लिए संपर्क करें

डॉ. अंबाती बुबली सागर
वैज्ञानिक - बी
एनआईसी, आंध्र प्रदेश राज्य इकाई, ए-ब्लॉक
तृतीय तल, आर एंड बी भवन, एम.जी. रोड, लब्बीपेट
विजयवाड़ा, आंध्र प्रदेश - 520010
ईमेल: sagar.ambati@nic.in, फ़ोन: 0866-2468371